

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-031956

(43)Date of publication of application : 28.01.2000

(51)Int.Cl.

H04L 9/08
G09C 1/00

(21)Application number : 10-200523

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

(22)Date of filing : 15.07.1998

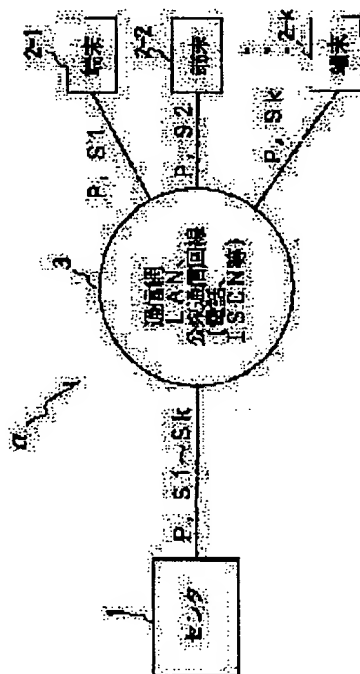
(72)Inventor : MINE SHINICHI
KAWAKITA TATSUJIRO
SAITO RYUICHI
NAKAHAMA KIYOSHI
YASUNAGA KENJI

(54) PERSONAL SECRET INFORMATION SHARED COMMUNICATION METHOD AND SYSTEM DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To share personal secret information at a low cost with security in common between a center and plurality of terminals without new installation of a communication line.

SOLUTION: This system is provided with a center 1 that stores common secret information P and personal secret information sets S1-Sk, discriminates legality of a request on the transmission request, encrypts the common secret information P or personal secret information sets S1-Sk and transmits the encrypted information, terminals 2-1-2-k that make transmission request of the common secret information P or the personal secret information sets S1-Sk to the center 1, decode the encrypted common secret information P or personal secret information sets S1-Sk sent from the center 1 and obtain the information, and a communication network 3 that interconnects the center 1 and the terminals 2-1-2-k.



LEGAL STATUS

[Date of request for examination]

27.10.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-31956

(P2000-31956A)

(43) 公開日 平成12年1月28日 (2000.1.28)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 B 5 K 0 1 3
G 0 9 C 1/00	6 3 0	G 0 9 C 1/00	6 3 0 B
	6 4 0		6 4 0 B

審査請求 未請求 請求項の数45 O L (全 23 頁)

(21) 出願番号 特願平10-200523

(22) 出願日 平成10年7月15日 (1998.7.15)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 嶺 真一

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72) 発明者 川北 達次郎

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(74) 代理人 100071113

弁理士 菅 隆彦

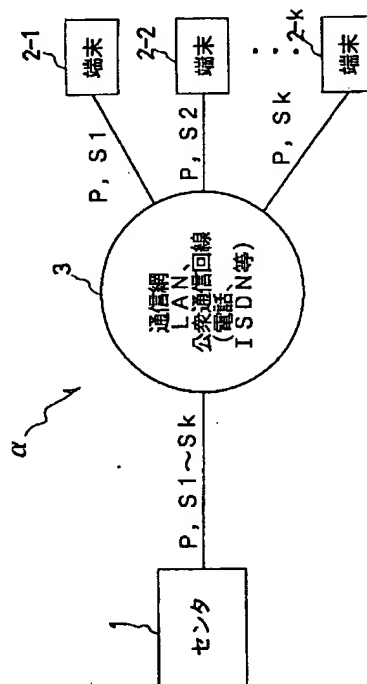
最終頁に続く

(54) 【発明の名称】 個別秘密情報共有通信方法及びシステム装置

(57) 【要約】

【課題】センタと複数の端末との間で、新しく通信回線を設置することなく、安全で安価に個別秘密情報を共有することができる個別秘密情報共有通信方法及びシステム装置の提供。

【解決手段】共通秘密情報P及び個別秘密情報S1～Skを蓄積しその要求がある場合に当該要求が正常であることを判断して共通秘密情報P又は個別秘密情報S1～Skを暗号化して送信するセンタ1と、センタ1へ共通秘密情報P又は個別秘密情報S1～Skの要求を行いセンタ1から送信された暗号化された共通秘密情報P又は個別秘密情報S1～Skを復号化して得る端末2-1～2-kと、センタ1及び各端末2-1～2-kを接続する通信網3とを備える特徴。



【特許請求の範囲】

【請求項1】通信網を介して複数の端末とセンタ間においてセキュリティシステム通信を行うに当り、
予め、当該複数の端末と当該センタ相互で、当該センタに共通の共通秘密情報及び当該各端末に個々の個別秘密情報を蓄積し合い、

前記各端末から通信リクエストを前記通信網を介して受けた前記センタは、その通信リクエストが正常であるかをその都度判断した上で前記共通秘密情報又は前記個別秘密情報ともども返信レポートを含め暗号化して前記通信網を介し送信する一方、

前記センタから返信を受けた前記各端末は、送信されかつ暗号化された前記返信レポートともども復号化する前記共通秘密情報又は前記個別秘密情報を抽出消去する、
ことを特徴とする個別秘密情報共有通信方法。

【請求項2】前記通信リクエストは、
前記各端末で暗号化され、前記センタで復号化される、
ことを特徴とする請求項1に記載の個別秘密情報共有通信方法。

【請求項3】前記複数の端末は、
前記通信網を介し相互に通信可能とする、
ことを特徴とする請求項1又は2に記載の個別秘密情報共有通信方法。

【請求項4】通信網で接続された複数の端末とセンタ間においてセキュリティシステム通信を行うために、当該センタから前記複数の端末のうちの送信対象の端末へ、前記各端末で固有の秘密情報である個別秘密情報の送信を行うに当り、

前記センタにおいて、
当該センタに蓄積された前記個別秘密情報を、同じく当該センタに蓄積されて前記各端末で共通な秘密情報である前記共通秘密情報で暗号化をして暗号化個別秘密情報を作成し、当該暗号化秘密情報を含む第1のレポートを前記送信対象の端末へ前記通信網を介して送信し、

次に前記送信対象の端末において、
前記第1のレポートを受信し、当該端末に蓄積していた前記共通秘密情報で復号化をして前記個別秘密情報を取り出し、当該個別秘密情報の受信が正常完了したか否かを示す結果である第1のレポート受信結果を作成し、当該第1のレポート受信結果が正常を意味する場合に、当該端末に蓄積していた前記共通秘密情報を消去する、
ことを特徴とする個別秘密情報共有通信方法。

【請求項5】前記個別秘密情報の送信は、
その前に、前記送信対象の端末から前記センタへ前記個別秘密情報の要求を行い、その際、
前記送信対象の端末において、

当該端末に蓄積されて前記センタが前記各端末を識別可能な情報である端末情報を、同じく当該端末に蓄積された前記共通秘密情報で暗号化したものにより第1の署名情報を作成し、当該第1の署名情報を含むメッセージ

である第1のリクエストを前記通信網を介して送信し、次に前記センタにおいて、

前記第1のリクエストを受信し前記第1の署名情報を取り出し、当該センタに蓄積された前記共通秘密情報で復号化をして前記第1の署名情報に含まれる前記端末情報を取り出し当該第1の署名情報の正当性の認証をした結果である第1の認証結果を作成し、当該第1の認証結果が正常である場合に、前記送信対象の端末である前記端末情報に示された端末へ前記第1のレポートの送信指示を行う、

ことを特徴とする請求項4に記載の個別秘密情報共有通信方法。

【請求項6】前記個別秘密情報の要求は、
前記第1の署名情報の作成に際し、
前記端末情報に加えて、当該送信対象の端末に蓄積されて前記第1の署名情報を作成する度に毎回異なる値である第1の署名識別子を、前記共通秘密情報で暗号化をして前記第1の署名情報の作成をし、

前記第1のレポートの送信指示に際し、
前記第1のリクエストを受信し第1の署名情報を取り出し、前記共通秘密情報で復号化をして前記第1の署名情報に含まれる前記端末情報及び前記第1の署名識別子を取り出し、当該第1の署名情報の正当性の認証をした結果である第1の認証結果を作成し、また取出された前記第1の署名識別子が過去に既に使用済みか否かを示す結果である第1の確認結果を作成し、前記第1の認証結果が正常で、前記第1の確認結果が未使用の場合に行う、
ことを特徴とする請求項5に記載の個別秘密情報共有通信方法。

【請求項7】前記第1の署名情報の作成は、
前記端末情報及び前記第1の署名識別子を前記共通秘密情報で暗号化したものに、当該端末情報及び当該第1の署名識別子を付加して行い、
前記第1の認証結果の正当性の認証は、
前記端末情報及び前記第1の署名識別子を前記共通秘密情報で暗号化したものを復号化した復号化端末情報及び復号化第1の署名識別子と、付加された前記端末情報及び前記第1の署名識別子とを比較して、一致する場合に正常であると認証する、

ことを特徴とする請求項6に記載の個別秘密情報共有通信方法。

【請求項8】前記個別秘密情報の送信は、
その後、前記センタから前記送信対象の端末へ前記共通秘密情報の要求を行い、その際、
前記センタにおいて、

当該センタに蓄積された前記共通秘密情報を、同じく当該センタに蓄積された前記個別秘密情報で暗号化をして暗号化共通秘密情報を作成し、当該暗号化共通秘密情報を含む第2のレポートを送信対象の前記端末へ前記通信網を介して送信し、

次に前記送信対象の端末において、
前記第2のレポートを受信し、当該端末に蓄積していた前記個別秘密情報で復号化をして前記共通秘密情報を取り出し、当該共通秘密情報の受信が正常完了したか否かを示す結果である第2のレポート受信結果を作成し、当該第2のレポート受信結果が正常を意味する場合に、当該端末に蓄積していた前記個別秘密情報を消去する、
ことを特徴とする請求項4、5、6又は7に記載の個別秘密情報共有送信方法。

【請求項9】前記共通秘密情報の送信は、
その前に、前記送信対象の端末から前記センタへ前記共通秘密情報の要求を行い、その際、
前記送信対象の端末において、
当該端末に蓄積された前記端末情報を、同じく当該端末に蓄積された前記個別秘密情報で暗号化したものにより第2の署名情報を作成し、当該第2の署名情報を含むメッセージである第2のリクエストを前記通信網を介して送信し、
次に前記センタにおいて、
前記第2のリクエストを受信し前記第2の署名情報を取り出し、当該センタに蓄積された前記個別秘密情報で復号化をして前記第2の署名情報に含まれる前記端末情報を取り出し当該第2の署名情報の正当性を認証した結果である第1の認証結果を作成し、当該第2の認証結果が正常である場合に、前記送信対象の端末である前記端末情報に示された端末へ前記第2のレポートの送信指示を行う、
ことを特徴とする請求項8に記載の個別秘密情報共有送信方法。

【請求項10】前記共通秘密情報の要求は、
前記第2の署名情報の作成に際し、
前記端末情報に加えて、当該送信対象の端末に蓄積されて前記第2の署名情報を作成する度に毎回異なる値である第2の署名識別子を、前記個別秘密情報で暗号化をして前記第2の署名情報の作成をし、
前記第2のレポートの送信指示に際し、
前記第2のリクエストを受信し前記第2の署名情報を取り出し、前記個別秘密情報で復号化をして前記第2の署名情報に含まれる前記端末情報及び前記第2の署名識別子を取り出し、当該第2の署名情報の正当性を認証した結果である第2の認証結果を作成し、また取出された前記第2の署名識別子が過去に既に使用済みか否かを示す結果である第2の確認結果を作成し、前記第2の認証結果が正常で、前記第2の確認結果が未使用の場合に行う、
ことを特徴とする請求項9に記載の個別秘密情報共有送信方法。

【請求項11】前記第2の署名情報の作成は、
前記端末情報及び前記第2の署名識別子を前記個別秘密情報で暗号化したものに、当該端末情報及び当該第2の署名識別子を付加して行い、

前記第2の認証結果の正当性の認証は、
前記端末情報及び前記第2の署名識別子を前記共通秘密情報で暗号化したものを復号化した復号化端末情報及び復号化第2の署名識別子と、付加された前記端末情報及び前記第2の署名識別子とを比較して、一致する場合に正常であると認証する、
ことを特徴とする請求項10に記載の個別秘密情報共有送信方法。

【請求項12】前記暗号化は、
既知平文攻撃に十分な耐性のある暗号化関数を用いて行う、
ことを特徴とする請求項1、2、3、4、5、6、7、8、9、10又は11に記載の個別秘密情報共有送信方法。

【請求項13】前記端末情報は、
前記各端末で重複しないものであり、
前記各端末が接続されている前記通信網におけるアドレス及び前記各端末で連続な連続番号を含める、
ことを特徴とする請求項5、6、7、8、9、10、11又は12に記載の個別秘密情報共有送信方法。

【請求項14】前記第1の署名識別子は、
前記第1の署名情報を作成する度にカウントアップする番号及び乱数を含める、
ことを特徴とする請求項6、7、8、9、10、11、12又は13に記載の個別秘密情報共有送信方法。

【請求項15】前記第2の署名識別子は、
前記第2の署名情報を作成する度にカウントアップする番号及び乱数を含める、
ことを特徴とする請求項10、11、12、13又は14に記載の個別秘密情報共有送信方法。

【請求項16】前記個別秘密情報は、
前記各端末間で固有の秘密情報である端末間秘密情報を含む、
ことを特徴とする請求項3、4、5、6、7、8、9、10、11、12、13、14又は15に記載の個別秘密情報共有送信方法。

【請求項17】前記個別秘密情報は、
変更可能なものであり、
時間関数及び設定自在なパラメータである世代識別子の関数を含める、
ことを特徴とする請求項1、2、3、4、5、6、7、8、9、10、11、12、13、14、15又は16に記載の個別秘密情報共有送信方法。

【請求項18】前記共通秘密情報は、
変更可能なものであり、
時間関数及び設定自在なパラメータである世代識別子の関数を含める、
ことを特徴とする請求項1、2、3、4、5、6、7、8、9、10、11、12、13、14、15、16又は

は17に記載の個別秘密情報共有送信方法。

【請求項19】前記個別秘密情報及び前記共通秘密情報は、

それぞれ、

前記暗号化を行う場合には、暗号鍵を含み、

前記認証を行う場合には、ユーザ名及びパスワード等を含み、

前記セキュリティ通信時に使用する前記通信網中の通信回線及び前記センタ及び前記各端末のポートを特定する場合には、当該通信回線及び当該ポートの情報を含む、ことを特徴とする請求項1、2、3、4、5、6、7、8、9、10、11、12、13、14、15、16、17又は18に記載の個別秘密情報共有送信方法。

【請求項20】前記通信網は、

LANや、電話及びISDNを含む公衆通信回線のうちの少なくとも1つからなる、

ことを特徴とする請求項1、2、3、4、5、6、7、8、9、10、11、12、13、14、15、16、17、18又は19に記載の個別秘密情報共有送信方法。

【請求項21】前記送信は、

前記通信網が公衆通信回線である場合に、

最初に、送信側から受信側へ発呼動作を行い、回線接続が完了した後の確保された通信チャンネル上で行う、

ことを特徴とする請求項20に記載の個別秘密情報共有送信方法。

【請求項22】通信網に接続された複数の端末と、当該複数の各端末と前記通信網を介して接続し当該各端末で固有の秘密情報である個別秘密情報を共有するセンタとを有する個別秘密情報システム装置であって、

前記センタは、

前記各端末で共通に用いる秘密情報である共通秘密情報を蓄積する共通秘密情報センタ蓄積手段と、

前記全端末の前記個別秘密情報を蓄積する個別秘密情報センタ蓄積手段と、

前記個別秘密情報の前記各端末への送信指示を行う個別秘密情報送信指示手段と、

当該個別秘密情報送信指示手段からの送信指示に従い、

前記個別秘密情報センタ蓄積手段に蓄積された前記個別秘密情報を、前記共通秘密情報センタ蓄積手段に蓄積された前記共通秘密情報で暗号化する暗号化個別秘密情報を含むメッセージである第1のレポートを作成し前記各端末に前記通信網を介して送信する第1のレポート作成送信手段とを有する、

ことを特徴とする個別秘密情報共有送信システム装置。

【請求項23】前記各端末は、

前記共通秘密情報を蓄積する共通秘密情報端末蓄積手段と、

前記センタから送信される前記第1のレポートを受信し当該第1のレポートに含まれる前記暗号化個別秘密情報

を、前記共通秘密情報端末蓄積手段に蓄積された前記共通秘密情報で復号化し前記個別秘密情報を取り出すとともに、当該個別秘密情報の受信が正常完了したか否かを示す結果である第1のレポート受信結果を作成する第1のレポート受信解析手段と、

当該第1のレポート受信解析手段で取出された前記個別秘密情報を蓄積する個別秘密情報端末蓄積手段と、

前記第1のレポート受信解析手段で作成された前記第1のレポート受信結果が正常を意味する場合に、前記共通秘密情報端末蓄積手段で蓄積している前記共通秘密情報を消去する共通秘密情報消去手段とを有する、

ことを特徴とする請求項22に記載の個別秘密情報共有送信システム装置。

【請求項24】前記各端末は、

前記センタで前記各端末それぞれを識別可能とする情報である端末情報を蓄積する端末情報蓄積手段と、

当該端末情報蓄積手段に蓄積された当該端末情報を、前記共通秘密情報端末蓄積手段に蓄積された前記共通秘密情報とを用いて暗号化をして第1の署名情報を作成する第1の署名情報作成手段と、

前記センタに対して前記個別秘密情報を含む前記第1のレポートの送信要求を行うために、前記第1の署名情報作成手段で作成された前記第1の署名情報を含むメッセージである第1のリクエストを作成し、前記センタに前記通信網を介して送信する第1のリクエスト作成送信手段とを有する、

ことを特徴とする請求項22又は23に記載の個別秘密情報共有送信システム装置。

【請求項25】前記センタは、

前記端末から送信される前記第1のリクエストを受信し、当該第1のリクエストに含まれる前記第1の署名情報を取出す第1のリクエスト受信解析手段と、

前記共通秘密情報センタ蓄積手段に蓄積された前記共通秘密情報を用いて復号化をして、前記第1のリクエスト受信解析手段で取出された前記第1の署名情報に含まれる前記端末情報を取出し、当該第1の署名情報の正当性を認証した結果である第1の認証結果を作成する第1の署名情報認証手段とを有し、

前記第1の個別秘密情報送信指示手段は、

前記第1の署名情報認証手段で作成された前記第1の認証結果が正常の場合に、前記第1の署名情報認証手段で取出された前記第1の端末情報に示される端末への第1のレポートの送信指示を前記第1のレポート作成送信手段に対して行う機能を有する、

ことを特徴とする請求項24に記載の個別秘密情報共有送信システム装置。

【請求項26】前記各端末は、

前記第1の署名情報を作成する度に毎回異なる値である第1の署名識別子を作成する第1の署名識別子作成手段を有し、

前記第1の署名情報作成手段は、
前記端末情報蓄積手段に蓄積された前記端末情報と、前記第1の署名識別子作成手段で作成された前記第1の署名識別子とを、前記共通秘密情報端末蓄積手段に蓄積された前記共通秘密情報を用いて暗号化をして前記第1の署名情報を作成する機能を有する、
ことを特徴とする請求項24又は25に記載の個別秘密情報共有通信システム装置。

【請求項27】前記第1の署名情報認証手段は、
前記共通情報センタ蓄積手段に蓄積された前記共通秘密情報を用いて復号化をして、前記第1のリクエスト情報受信解析手段で取出された前記第1の署名情報から前記端末情報及び前記第1の署名識別子を取り出し前記第1の署名情報の正当性を認証した第1の認証結果を作成する機能を有し、

前記センタは、

前記第1の署名情報認証手段で取出された前記第1の署名識別子が過去に既に使用済みか否かを示す結果である第1の確認結果を作成する第1の署名識別子使用状況確認手段を有し、

前記第1の個別秘密情報送信指示手段は、

前記第1の署名情報認証手段で作成された前記第1の認証結果が正常でかつ、前記第1の署名識別子使用状況確認手段で取出された前記第1の確認結果が未使用の場合に、前記第1の署名識別子使用状況確認手段で取出された前記端末情報に示される端末への前記第1のレポートの送信指示を、前記第1のレポート作成送信手段に対して行う機能を有する、

ことを特徴とする請求項26に記載の個別秘密情報共有通信システム装置。

【請求項28】前記センタは、

前記共通秘密情報の前記各端末への送信指示を行う共通秘密情報送信指示手段と、

当該共通秘密情報送信指示手段からの送信指示に従い、前記共通秘密情報センタ蓄積手段に蓄積された前記共通秘密情報を、前記個別秘密情報センタ蓄積手段に蓄積された前記個別秘密情報で暗号化する暗号化共通秘密情報を含むメッセージである第2のレポートを作成し前記各端末に前記通信網を介して送信する第2のレポート作成送信手段とを有する、

ことを特徴とする請求項22、23、24、25、26又は27に記載の個別秘密情報共有通信システム装置。

【請求項29】前記各端末は、

前記センタから送信される前記第2のレポートを受信し当該第2のレポートに含まれる前記暗号化共通秘密情報を、前記個別秘密情報端末蓄積手段に蓄積された前記個別秘密情報で復号化し前記共通秘密情報を取出すとともに、当該共通秘密情報の受信が正常完了したか否かを示す結果である第2のレポート受信結果を作成する第2のレポート受信解析手段と、

当該第2のレポート受信解析手段で作成された前記第2のレポート受信結果が正常を意味する場合に、前記個別秘密情報端末蓄積手段に蓄積している前記個別秘密情報を消去する個別秘密情報消去手段とを有し、

前記共通秘密情報端末蓄積手段は、

前記第2のレポート受信解析手段で取出された前記共通秘密情報を蓄積する機能も有する、

ことを特徴とする請求項28に記載の個別秘密情報共有通信システム装置。

【請求項30】前記各端末は、

前記端末情報蓄積手段に蓄積された前記端末情報を、前記個別秘密情報端末蓄積手段に蓄積された前記個別秘密情報を用いて暗号化をして第2の署名情報を作成する第2の署名情報作成手段と、

前記センタに対して前記共通秘密情報を含む前記第2のレポートの送信要求を行うために、前記第2の署名情報作成手段で作成された前記第2の署名情報を含むメッセージである第2のリクエストを作成し、前記センタに前記通信網を介して送信する第2のリクエスト作成送信手段とを有する、

ことを特徴とする請求項28又は29に記載の個別秘密情報共有通信システム装置。

【請求項31】前記センタは、

前記端末から送信される前記第2のリクエストを受信し、当該第2のリクエストに含まれる前記署名情報を取出す第2のリクエスト受信解析手段と、

前記個別秘密情報センタ蓄積手段に蓄積された前記個別秘密情報を用いて復号化をして、前記第2のリクエスト受信解析手段で取出された前記第2の署名情報に含まれる前記端末情報を取出し、当該第2の署名情報の正当性を認証した結果である第2の認証結果を作成する第2の署名情報認証手段とを有し、

前記共通秘密情報送信指示手段は、

前記第2の署名情報認証手段で作成された前記第2の認証結果が正常の場合に、前記第2の署名情報認証手段で取出された前記端末情報に示される端末への第2のレポートの送信指示を前記第2のレポート作成送信手段に対して行う機能を有する、

ことを特徴とする請求項30に記載の個別秘密情報共有通信システム装置。

【請求項32】前記各端末は、

前記第2の署名情報を作成する度に毎回異なる値である第2の署名識別子を作成する第2の署名識別子作成手段を有し、

前記第2の署名情報作成手段は、

前記端末情報蓄積手段に蓄積された前記端末情報と、前記第2の署名識別子作成手段で作成された前記第2の署名識別子とを、前記個別秘密情報端末蓄積手段に蓄積された前記個別秘密情報を用いて暗号化して、前記第2の署名情報を作成する機能を有する、

ことを特徴とする請求項30又は31に記載の個別秘密情報共有通信システム装置。

【請求項33】前記第2の署名情報認証手段は、前記個別秘密情報センタ蓄積手段に蓄積された前記個別秘密情報を用いて復号化して、前記第2のリクエスト情報受信解析手段で取出された前記第2の署名情報から前記端末情報及び前記第2の署名識別子を取り出し前記第2の署名情報の正当性を認証した第2の認証結果を作成する機能を有し、

前記センタは、

前記第2の署名情報認証手段で取出された前記第2の署名識別子が過去に既に使用済みか否かを示す結果である第2の確認結果を作成する第2の署名識別子使用状況確認手段を有し、

前記共通秘密情報送信指示手段は、

前記第2の署名情報認証手段で作成された前記第2の認証結果が正常でかつ、前記第2の署名識別子使用状況確認手段で取出された前記第2の確認結果が未使用の場合に、前記第2の署名識別子使用状況確認手段で取出された前記端末情報に示される端末への前記第2のレポートの送信指示を、前記第2のレポート作成送信手段に対して行う機能を有する、

ことを特徴とする請求項32に記載の個別秘密情報共有通信システム装置。

【請求項34】前記個別秘密情報送信指示手段は、

前記共通秘密情報の前記各端末への送信指示を行う機能も有し、

前記第1のレポート作成送信手段は、

当該個別秘密情報送信指示手段からの送信指示に従い、前記共通秘密情報センタ蓄積手段に蓄積された前記共通秘密情報を、前記個別秘密情報センタ蓄積手段に蓄積された前記個別秘密情報で暗号化する暗号化共通秘密情報を含むメッセージである第2のレポートを作成し前記各端末に前記通信網を介して送信する機能も有する、

ことを特徴とする請求項22、23、24、25、26又は27に記載の個別秘密情報共有通信システム装置。

【請求項35】前記第1のレポート受信解析手段は、

前記センタから送信される前記第2のレポートを受信し当該第2のレポートに含まれる前記暗号化共通秘密情報を、前記個別秘密情報端末蓄積手段に蓄積された前記個別秘密情報で復号化し前記共通秘密情報を取出すとともに、当該共通秘密情報の受信が正常完了したか否かを示す結果である第2のレポート受信結果を作成する機能も有し、

前記共通秘密情報消去手段は、

当該第1のレポート受信解析手段で作成された前記第2のレポート受信結果が正常を意味する場合に、前記個別秘密情報端末蓄積手段で蓄積している前記個別秘密情報を消去する機能も有し、

前記共通秘密情報端末蓄積手段は、

前記第1のレポート受信解析手段で取出された前記共通秘密情報を蓄積する機能も有する、

ことを特徴とする請求項34に記載の個別秘密情報共有通信システム装置。

【請求項36】前記第1の署名情報作成手段は、

前記端末情報蓄積手段に蓄積された前記端末情報と、前記個別秘密情報端末蓄積手段に蓄積された前記個別秘密情報とを用いて暗号化して第2の署名情報を作成する機能も有し、

前記第1のリクエスト作成送信手段は、

前記センタに対して前記共通秘密情報を含む前記第2のレポートの送信要求を行うために、前記第2の署名情報作成手段で作成された前記第2の署名情報を含むメッセージである第2のリクエストを作成し、前記センタに前記通信網を介して送信する機能も有する、

ことを特徴とする請求項34又は35に記載の個別秘密情報共有通信システム装置。

【請求項37】前記第1のリクエスト受信解析手段は、

前記端末から送信される前記第2のリクエストを受信し、当該第2のリクエストに含まれる前記署名情報を取り出す機能も有し、

第1の署名情報認証手段は、

前記個別秘密情報センタ蓄積手段に蓄積された前記個別秘密情報を用いて、前記第2のリクエスト受信解析手段で取出された前記第2の署名情報に含まれる前記端末情報を取り出し、当該第2の署名情報の正当性を認証した結果である第2の認証結果を作成する機能も有し、

前記個別秘密情報送信指示手段は、

前記第1の署名情報認証手段で作成された前記第2の認証結果が正常の場合に、前記第1の署名情報認証手段で取出された前記端末情報に示される端末への第2のレポートの送信指示を前記第1のレポート作成送信手段に対して行う機能も有する、

ことを特徴とする請求項36に記載の個別秘密情報共有通信システム装置。

【請求項38】前記第1の署名識別子作成手段は、

前記第2の署名情報を作成する度に毎回異なる値である第2の署名識別子を作成する機能も有し、

前記第1の署名情報作成手段は、

前記端末情報蓄積手段に蓄積された前記端末情報と、前記第2の署名識別子作成手段で作成された前記第2の署名識別子とを、前記個別秘密情報端末蓄積手段に蓄積された前記個別秘密情報を用いて暗号化をして、前記第2の署名情報を作成する機能も有する、

ことを特徴とする請求項36又は37に記載の個別秘密情報共有通信システム装置。

【請求項39】前記第1の署名情報認証手段は、

前記個別秘密情報センタ蓄積手段に蓄積された前記個別秘密情報を用いて復号化をして、前記第1のリクエスト情報受信解析手段で取出された前記第2の署名情報から前記

端末情報及び前記第2の署名識別子を取り出し前記第2の署名情報の正当性を認証した第2の認証結果を作成する機能も有し、

前記第1の署名識別子使用状況確認手段は、

前記第1の署名情報認証手段で取出された前記第2の署名識別子が過去に既に使用済みか否かを示す結果である第2の確認結果を作成する第2の署名識別子使用状況確認手段を有し、

前記個別秘密情報送信指示手段は、

前記第1の署名情報認証手段で作成された前記第2の認証結果が正常でかつ、前記第1の署名識別子使用状況確認手段で取出された前記第2の確認結果が未使用の場合に、前記第1の署名識別子使用状況確認手段で取出された前記端末情報に示される端末への前記第2のレポートの送信指示を、前記第2のレポート作成送信手段に対して行う機能も有する、

ことを特徴とする請求項38に記載の個別秘密情報共有通信システム装置。

【請求項40】前記通信網は、

LANや、電話及びISDNを含む公衆通信回線のうちの少なくとも1つからなる、

ことを特徴とする請求項22、23、24、25、26、27、28、29、30、31、32、33、34、35、36、37、38又は39に記載の個別秘密情報共有通信システム装置。

【請求項41】前記センタは、

前記共通秘密情報及び前記個別秘密情報を共有しセキュリティ通信を行うセキュリティ通信部を有する、

ことを特徴とする請求項22、23、24、25、26、27、28、29、30、31、32、33、34、35、36、37、38、39又は40に記載の個別秘密情報共有通信システム装置。

【請求項42】前記センタとは別に、

前記共通秘密情報及び前記個別秘密情報を共有しセキュリティ通信を行うセキュリティ通信装置を設ける、

ことを特徴とする請求項22、23、24、25、26、27、28、29、30、31、32、33、34、35、36、37、38、39又は40に記載の個別秘密情報共有通信システム装置。

【請求項43】前記センタ及び前記各端末は、

別に、前記共通秘密情報を時間関数及び設定自在なパラメータとする世代識別子の関数を入力及び蓄積する鍵注入器を設ける、

ことを特徴とする請求項22、23、24、25、26、27、28、29、30、31又は32に記載の個別秘密情報共有通信システム装置。

【請求項44】前記第1の署名識別子作成手段は、

前記第1の署名情報を作成する度にカウントアップするカウンタ及び乱数を発生するプログラムのうちの1つを有する、

ことを特徴とする請求項26、27、28、29、30、31、32、33、34、35、36、37、38、39、40、41、42又は43に記載の個別秘密情報共有通信システム装置。

【請求項45】前記第2の署名識別子は、

前記第2の署名情報を作成する度にカウントアップするカウンタ及び乱数を発生するプログラムのうちの1つを有する、

ことを特徴とする請求項32、33、38、39、40、41、42、43又は44に記載の個別秘密情報共有通信システム装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】センタと端末間でLANや公衆通信回線等のように予め不正アクセスやデータ不正モニタの防止機能が十分具備されていない通信回線を用いてセキュリティ通信を行う通信システムにおいて、前記通信回線を用いてセンタと各端末間で各端末毎に異なる個別秘密情報を共有可能とする個別秘密情報共有通信方法及びその実施に直接用いるシステム装置に関するものである。

【0002】

【従来の技術】遠隔地に設置された複数の端末とセンタの間で、LANや、電話、ISDN等の公衆通信回線を介して各種通信を行うシステムにおいて、その機能を安定して確実に動作させるためには、不正者によるセンタのアクセスや回線上で伝送される信号の盗聴等によるハッキング対策として、何らかのセキュリティ上の保護機能を具備しておく必要がある。

【0003】このセキュリティ機能を実現するためには、センタと端末が自身の正当性を証明することが可能な（不正者が持ち得ない）秘密情報を共有しアクセス開始時に相互認証を行ったり、転送データの暗号化を行う方法が有効であるが、これを実現するためには、セキュリティ通信を通信を開始する前の段階で、各端末とセンタで同一の秘密情報を共有しておく必要がある。

【0004】また、万一いずれかの端末から秘密情報が漏洩した場合に、他の端末の通信に与える影響を極力小さくするという観点からは、セキュリティ通信に用いる秘密情報は各端末毎に異なる秘密情報である個別秘密情報とすることが望ましい。

【0005】従来は、センタと各端末の間で個別秘密情報を共有するためには、センタと端末間で安全に情報を配送できる高セキュリティ機能を具備した通信手段（例えば、信頼できる人を介して直接双方に入力したり、郵便書留等のような親展通信を用いる等）を介して、秘密情報を入力する方法が用いられている。

【0006】

【発明が解決しようとする課題】しかし、上記従来技術では、端末とセンタ間でLANや公衆通信回線等のよう

に予め不正アクセスやデータ不正モニタの防止機能が十分具備されていない通信回線を用いてセキュリティ通信を行おうとすると、センタと各端末間で個別秘密情報を共有するために別の高価な(かつ安全な)通信手段が必要となるため、センタに収束する端末数が多かったりその設置場所が多岐にわたっているような場合には、経済的にセキュリティ通信システムを実現することが難しいという問題点があった。

【0007】また、これを解決するために各端末に共通な秘密情報である共通秘密情報を用いて、センタと各端末間でセキュリティ通信を行おうとすると、万一上記秘密情報が漏洩した場合には、システム全体に影響が及ぶという別の問題点があった。

【0008】ここにおいて、本発明の解決すべき主要な目的は次の通りである。

【0009】本発明の第1の目的は、センタと各端末間で経済的に安価でかつ安全に個別秘密情報を共有することができる個別秘密情報共有交通方法及びシステム装置を提供せんとするものである。

【0010】本発明の第2の目的は、センタと各端末間で別の新たな通信回線を設置しなくてもよい個別秘密情報共有交通方法及びシステム装置を提供せんとするものである。

【0011】本発明の第3の目的は、万一共通秘密情報が漏洩した場合にもシステム全体に影響が及ぶことのない個別秘密情報交通共有方法及びシステム装置を提供せんとするものである。

【0012】本発明のその他の目的は、明細書、図面、特に特許請求の範囲の各請求項の記載から自ずと明らかとなる。

【0013】

【課題を解決するための手段】本発明は、上記課題の解決に当たり、複数の端末とセンタとを通信網で接続して当該センタにおいて個別秘密情報及び共通秘密情報を共有交通する装置の特徴を有し、前記センタにおいて前記個別秘密情報を前記共通秘密情報で暗号化して送信し、前記各端末において前記暗号化した個別秘密情報を前記共通秘密情報で復号化して前記共通秘密情報を得る方法の特徴を有する。

【0014】更に具体的詳細に述べると、当該課題の解決では、本発明が次に列挙する上位概念から下位概念に互る新規な特徴的構成手段又は手法を採用することにより、前記目的を達成するよう為される。

【0015】即ち、本発明方法の第1の特徴は、通信網を介して複数の端末とセンタ間においてセキュリティシステム交通を行うに当り、予め、当該複数の端末と当該センタ相互で、当該センタに共通の共通秘密情報及び当該各端末に固有の個別秘密情報を蓄積し合い、前記各端末から交通リクエストを前記通信網を介して受けた前記センタは、その交通リクエストが正常であるかをその都

度判断した上で前記共通秘密情報又は前記個別秘密情報ともども返信レポートを含め暗号化して前記通信網を介し送信する一方、前記センタから返信を受けた前記各端末は、送信されかつ暗号化された前記返信レポートともども復号化する前記共通秘密情報又は前記個別秘密情報を抽出消去してなる個別秘密情報共有交通方法の構成採用にある。

【0016】本発明方法の第2の特徴は、上記本発明方法の第1の特徴における前記交通リクエストが、前記各端末で暗号化され、前記センタで復号化されてなる個別秘密情報共有交通方法の構成採用にある。

【0017】本発明方法の第3の特徴は、上記本発明方法の第1又は第2の特徴における前記複数の端末が、前記通信網を介し相互に交通可能としてなる個別秘密情報共有交通方法の構成採用にある。

【0018】本発明方法の第4の特徴は、通信網で接続された複数の端末とセンタ間においてセキュリティシステム交通を行うために、当該センタから前記複数の端末のうちの送信対象の端末へ、前記各端末で固有の秘密情報である個別秘密情報の送信を行うに当り、前記センタにおいて、当該センタに蓄積された前記個別秘密情報を、同じく当該センタに蓄積されて前記各端末で共通な秘密情報である前記共通秘密情報で暗号化をして暗号化個別秘密情報を作成し、当該暗号化秘密情報を含む第1のレポートを前記送信対象の端末へ前記通信網を介して送信し、次に前記送信対象の端末において、前記第1のレポートを受信し、当該端末に蓄積していた前記共通秘密情報で復号化をして前記個別秘密情報を取出し、当該個別秘密情報の受信が正常完了したか否かを示す結果である第1のレポート受信結果を作成し、当該第1のレポート受信結果が正常を意味する場合に、当該端末に蓄積していた前記共通秘密情報を消去してなる個別秘密情報共有交通方法の構成採用にある。

【0019】本発明方法の第5の特徴は、上記本発明方法の第4の特徴における前記個別秘密情報の送信が、その前に、前記送信対象の端末から前記センタへ前記個別秘密情報の要求を行い、その際、前記送信対象の端末において、当該端末に蓄積されて前記センタが前記各端末を識別可能な情報である端末情報を、同じく当該端末に蓄積された前記共通秘密情報で暗号化したものにより第1の署名情報を作成し、当該第1の署名情報を含むメッセージである第1のリクエストを前記通信網を介して送信し、次に前記センタにおいて、前記第1のリクエストを受信し前記第1の署名情報を取出し、当該センタに蓄積された前記共通秘密情報で復号化をして前記第1の署名情報に含まれる前記端末情報を取出し当該第1の署名情報の正当性の認証をした結果である第1の認証結果を作成し、当該第1の認証結果が正常である場合に、前記送信対象の端末である前記端末情報に示された端末へ前記第1のレポートの送信指示を行ってなる個別秘密情報

報共有通信方法の構成採用にある。

【0020】本発明方法の第6の特徴は、上記本発明方法の第5の特徴における前記個別秘密情報の要求が、前記第1の署名情報の作成に際し、前記端末情報に加えて、当該送信対象の端末に蓄積されて前記第1の署名情報を作成する度に毎回異なる値である第1の署名識別子を、前記共通秘密情報で暗号化をして前記第1の署名情報の作成をし、前記第1のレポートの送信指示に際し、前記第1のリクエストを受信し第1の署名情報を取出し、前記共通秘密情報で復号化をして前記第1の署名情報に含まれる前記端末情報及び前記第1の署名識別子を取出し、当該第1の署名情報の正当性の認証をした結果である第1の認証結果を作成し、また取出された前記第1の署名識別子が過去に既に使用済みか否かを示す結果である第1の確認結果を作成し、前記第1の認証結果が正常で、前記第1の確認結果が未使用の場合に行ってなる個別秘密情報共有通信方法の構成採用にある。

【0021】本発明方法の第7の特徴は、上記本発明方法の第6の特徴における前記第1の署名情報の作成が、前記端末情報及び前記第1の署名識別子を前記共通秘密情報で暗号化したものに、当該端末情報及び当該第1の署名識別子を付加して行い、前記第1の認証結果の正当性の認証が、前記端末情報及び前記第1の署名識別子を前記共通秘密情報で暗号化したものを復号化した復号化端末情報及び復号化第1の署名識別子と、付加された前記端末情報及び前記第1の署名識別子とを比較して、一致する場合に正常であると認証してなる個別秘密情報共有通信方法の構成採用にある。

【0022】本発明方法の第8の特徴は、上記本発明方法の第4、第5、第6又は第7の特徴における前記個別秘密情報の送信が、その後、前記センタから前記送信対象の端末へ前記共通秘密情報の要求を行い、その際、前記センタにおいて、当該センタに蓄積された前記共通秘密情報を、同じく当該センタに蓄積された前記個別秘密情報で暗号化をして暗号化共通秘密情報を作成し、当該暗号化共通秘密情報を含む第2のレポートを送信対象の前記端末へ前記通信網を介して送信し、次に前記送信対象の端末において、前記第2のレポートを受信し、当該端末に蓄積していた前記個別秘密情報で復号化をして前記共通秘密情報を取出し、当該共通秘密情報の受信が正常完了したか否かを示す結果である第2のレポート受信結果を作成し、当該第2のレポート受信結果が正常を意味する場合に、当該端末に蓄積していた前記個別秘密情報を消去してなる個別秘密情報共有通信方法の構成採用にある。

【0023】本発明方法の第9の特徴は、上記本発明方法の第8の特徴における前記共通秘密情報の送信が、その前に、前記送信対象の端末から前記センタへ前記共通秘密情報の要求を行いその際、前記送信対象の端末において、当該端末に蓄積された前記端末情報を、同じく当

該端末に蓄積された前記個別秘密情報で暗号化したものにより第2の署名情報を作成し、当該第2の署名情報を含むメッセージである第2のリクエストを前記通信網を介して送信し、次に前記センタにおいて、前記第2のリクエストを受信し前記第2の署名情報を取出し、当該センタに蓄積された前記個別秘密情報で復号化をして前記第2の署名情報に含まれる前記端末情報を取出し当該第2の署名情報の正当性を認証した結果である第1の認証結果を作成し、当該第2の認証結果が正常である場合に、前記送信対象の端末である前記端末情報に示された端末へ前記第2のレポートの送信指示を行ってなる個別秘密情報共有通信方法の構成採用にある。

【0024】本発明方法の第10の特徴は、上記本発明方法の第9の特徴における前記共通秘密情報の要求が、前記第2の署名情報の作成に際し、前記端末情報に加えて、当該送信対象の端末に蓄積されて前記第2の署名情報を作成する度に毎回異なる値である第2の署名識別子を、前記個別秘密情報で暗号化をして前記第2の署名情報の作成をし、前記第2のレポートの送信指示に際し、前記第2のリクエストを受信し前記第2の署名情報を取出し、前記個別秘密情報で復号化をして前記第2の署名情報に含まれる前記端末情報及び前記第2の署名識別子を取出し、当該第2の署名情報の正当性を認証した結果である第2の認証結果を作成し、また取出された前記第2の署名識別子が過去に既に使用済みか否かを示す結果である第2の確認結果を作成し、前記第2の認証結果が正常で、前記第2の確認結果が未使用の場合に行ってなる個別秘密情報共有通信方法の構成採用にある。

【0025】本発明方法の第11の特徴は、上記本発明方法の第10の特徴における前記第2の署名情報の作成が、前記端末情報及び前記第2の署名識別子を前記個別秘密情報で暗号化したものに、当該端末情報及び当該第2の署名識別子を付加して行い、前記第2の認証結果の正当性の認証が、前記端末情報及び前記第2の署名識別子を前記共通秘密情報で暗号化したものを復号化した復号化端末情報及び復号化第2の署名識別子と、付加された前記端末情報及び前記第2の署名識別子とを比較して、一致する場合に正常であると認証してなる個別秘密情報共有通信方法の構成採用にある。

【0026】本発明方法の第12の特徴は、上記本発明方法の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10又は第11の特徴における前記暗号化が、既知平文攻撃に十分な耐性のある暗号化関数を用いて行ってなる個別秘密情報共有通信方法の構成採用にある。

【0027】本発明方法の第13の特徴は、上記本発明方法の第5、第6、第7、第8、第9、第10、第11又は第12の特徴における前記端末情報が、前記各端末で重複しないものであり、前記各端末が接続されている前記通信網におけるアドレス及び前記各端末で連続な連

統番号を含めてなる個別秘密情報共有通信方法の構成採用にある。

【0028】本発明方法の第14の特徴は、上記本発明方法の第6、第7、第8、第9、第10、第11、第12又は第13の特徴における前記第1の署名識別子が、前記第1の署名情報を作成する度にカウントアップする番号及び乱数を含めてなる個別秘密情報共有通信方法の構成採用にある。

【0029】本発明方法の第15の特徴は、上記本発明方法の第10、第11、第12、第13又は第14の特徴における前記第2の署名識別子が、前記第2の署名情報を作成する度にカウントアップする番号及び乱数を含めてなる個別秘密情報共有通信方法の構成採用にある。

【0030】本発明方法の第16の特徴は、上記本発明方法の第3、第4、第5、第6、第7、第8、第9、第10、第11、第12、第13、第14又は第15の特徴における前記個別秘密情報が、前記各端末間で固有の秘密情報である端末間秘密情報を含んでなる個別秘密情報共有通信方法の構成採用にある。

【0031】本発明方法の第17の特徴は、上記本発明方法の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10、第11、第12、第13、第14、第15又は第16の特徴における前記個別秘密情報が、変更可能なものであり、時間関数及び設定自在なパラメータである世代識別子の関数を含めてなる個別秘密情報共有通信方法の構成採用にある。

【0032】本発明方法の第18の特徴は、上記本発明方法の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10、第11、第12、第13、第14、第15、第16又は第17の特徴における前記共通秘密情報が、変更可能なものであり、時間関数及び設定自在なパラメータである世代識別子の関数を含めてなる個別秘密情報共有通信方法の構成採用にある。

【0033】本発明方法の第19の特徴は、上記本発明方法の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10、第11、第12、第13、第14、第15、第16、第17又は第18の特徴における前記個別秘密情報及び前記共通秘密情報が、それぞれ、前記暗号化を行う場合には、暗号鍵を含み、前記認証を行う場合には、ユーザ名及びパスワード等を含み、前記セキュリティ通信時に使用する前記通信網中の通信回線及び前記センタ及び前記各端末のポートを特定する場合には、当該通信回線及び当該ポートの情報を含んでなる個別秘密情報共有通信方法の構成採用にある。

【0034】本発明方法の第20の特徴は、上記本発明方法の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10、第11、第12、第13、第14、第15、第16、第17、第18又は第19の特徴における前記通信網が、LANや、電話及びISDNを含む公衆通信回線のうちの少なくとも1つからなる個別秘密

情報共有通信方法の構成採用にある。

【0035】本発明方法の第21の特徴は、上記本発明方法の第20の特徴における前記送信が、前記通信網が公衆通信回線である場合に、最初に、送信側から受信側へ発呼動作を行い、回線接続が完了した後の確保された通信チャネル上で行ってなる個別秘密情報共有通信方法の構成採用にある。

【0036】本発明装置の第1の特徴は、通信網に接続された複数の端末と、当該複数の各端末と前記通信網を介して接続し当該各端末で固有の秘密情報である個別秘密情報を共有するセンタとを有する個別秘密情報システム装置であって、前記センタが、前記各端末で共通に用いる秘密情報である共通秘密情報を蓄積する共通秘密情報センタ蓄積手段と、前記全端末の前記個別秘密情報を蓄積する個別秘密情報センタ蓄積手段と、前記個別秘密情報の前記各端末への送信指示を行う個別秘密情報送信指示手段と、当該個別秘密情報送信指示手段からの送信指示に従い、前記個別秘密情報センタ蓄積手段に蓄積された前記個別秘密情報を、前記共通秘密情報センタ蓄積手段に蓄積された前記共通秘密情報で暗号化する暗号化個別秘密情報を含むメッセージである第1のレポートを作成し前記各端末に前記通信網を介して送信する第1のレポート作成送信手段とを有してなる個別秘密情報共有通信システム装置の構成採用にある。

【0037】本発明装置の第2の特徴は、上記本発明装置の第1の特徴における前記各端末が、前記共通秘密情報を蓄積する共通秘密情報端末蓄積手段と、前記センタから送信される前記第1のレポートを受信し当該第1のレポートに含まれる前記暗号化個別秘密情報を、前記共通秘密情報端末蓄積手段に蓄積された前記共通秘密情報で復号化し前記個別秘密情報を取出すとともに、当該個別秘密情報の受信が正常完了したか否かを示す結果である第1のレポート受信結果を作成する第1のレポート受信解析手段と、当該第1のレポート受信解析手段で取出された前記個別秘密情報を蓄積する個別秘密情報端末蓄積手段と、前記第1のレポート受信解析手段で作成された前記第1のレポート受信結果が正常を意味する場合には、前記共通秘密情報端末蓄積手段で蓄積している前記共通秘密情報を消去する共通秘密情報消去手段とを有してなる個別秘密情報共有通信システム装置の構成採用にある。

【0038】本発明装置の第3の特徴は、上記本発明装置の第1又は第2の特徴における前記各端末が、前記センタで前記各端末それぞれを識別可能とする情報である端末情報を蓄積する端末情報蓄積手段と、当該端末情報蓄積手段に蓄積された当該端末情報を、前記共通秘密情報端末蓄積手段に蓄積された前記共通秘密情報とを用いて暗号化をして第1の署名情報を作成する第1の署名情報作成手段と、前記センタに対して前記個別秘密情報を含む前記第1のレポートの送信要求を行うために、前記

第1の署名情報作成手段で作成された前記第1の署名情報を含むメッセージである第1のリクエストを作成し、前記センタに前記通信網を介して送信する第1のリクエスト作成送信手段とを有してなる個別秘密情報共有通信システム装置の構成採用にある。

【0039】本発明装置の第4の特徴は、上記本発明装置の第3の特徴における前記センタが、前記端末から送信される前記第1のリクエストを受信し、当該第1のリクエストに含まれる前記第1の署名情報を取出す第1のリクエスト受信解析手段と、前記共通秘密情報センタ蓄積手段に蓄積された前記共通秘密情報を用いて復号化をして、前記第1のリクエスト受信解析手段で取出された前記第1の署名情報に含まれる前記端末情報を取出し、当該第1の署名情報の正当性を認証した結果である第1の認証結果を作成する第1の署名情報認証手段とを有し、前記第1の個別秘密情報送信指示手段が、前記第1の署名情報認証手段で作成された前記第1の認証結果が正常の場合に、前記第1の署名情報認証手段で取出された前記第1の端末情報に示される端末への第1のレポートの送信指示を前記第1のレポート作成送信手段に対して行う機能を有してなる個別秘密情報共有通信システム装置の構成採用にある。

【0040】本発明装置の第5の特徴は、上記本発明装置の第3又は第4の特徴における前記各端末が、前記第1の署名情報を作成する度に毎回異なる値である第1の署名識別子を作成する第1の署名識別子作成手段を有し、前記第1の署名情報作成手段が、前記端末情報蓄積手段に蓄積された前記端末情報と、前記第1の署名識別子作成手段で作成された前記第1の署名識別子とを、前記共通秘密情報端末蓄積手段に蓄積された前記共通秘密情報を用いて暗号化をして前記第1の署名情報を作成する機能を有してなる個別秘密情報共有通信システム装置の構成採用にある。

【0041】本発明装置の第6の特徴は、上記本発明装置の第5の特徴における前記第1の署名情報認証手段が、前記共通情報センタ蓄積手段に蓄積された前記共通秘密情報を用いて復号化をして、前記第1のリクエスト情報受信解析手段で取出された前記第1の署名情報から前記端末情報及び前記第1の署名識別子を取り出し前記第1の署名情報の正当性を認証した第1の認証結果を作成する機能を有し、前記センタが、前記第1の署名情報認証手段で取出された前記第1の署名識別子が過去に既に使用済みか否かを示す結果である第1の確認結果を作成する第1の署名識別子使用状況確認手段を有し、前記第1の個別秘密情報送信指示手段が、前記第1の署名情報認証手段で作成された前記第1の認証結果が正常でかつ、前記第1の署名識別子使用状況確認手段で取出された前記第1の確認結果が未使用の場合に、前記第1の署名識別子使用状況確認手段で取出された前記端末情報に示される端末への前記第1のレポートの送信指示を、前

記第1のレポート作成送信手段に対して行う機能を有してなる個別秘密情報共有通信システム装置の構成採用にある。

【0042】本発明装置の第7の特徴は、上記本発明装置の第1、第2、第3、第4、第5又は第6の特徴における前記センタが、前記共通秘密情報の前記各端末への送信指示を行う共通秘密情報送信指示手段と、当該共通秘密情報送信指示手段からの送信指示に従い、前記共通秘密情報センタ蓄積手段に蓄積された前記共通秘密情報を、前記個別秘密情報センタ蓄積手段に蓄積された前記個別秘密情報で暗号化する暗号化共通秘密情報を含むメッセージである第2のレポートを作成し前記各端末に前記通信網を介して送信する第2のレポート作成送信手段とを有してなる個別秘密情報共有通信システム装置の構成採用にある。

【0043】本発明装置の第8の特徴は、上記本発明装置の第7の特徴における前記各端末が、前記センタから送信される前記第2のレポートを受信し当該第2のレポートに含まれる前記暗号化共通秘密情報を、前記個別秘密情報端末蓄積手段に蓄積された前記個別秘密情報で復号化し前記共通秘密情報を取出すとともに、当該共通秘密情報の受信が正常完了したか否かを示す結果である第2のレポート受信結果を作成する第2のレポート受信解析手段と、当該第2のレポート受信解析手段で作成された前記第2のレポート受信結果が正常を意味する場合に、前記個別秘密情報端末蓄積手段で蓄積している前記個別秘密情報を消去する個別秘密情報消去手段とを有し、前記共通秘密情報端末蓄積手段が、前記第2のレポート受信解析手段で取出された前記共通秘密情報を蓄積する機能も有してなる個別秘密情報共有システム装置の構成採用にある。

【0044】本発明装置の第9の特徴は、上記本発明装置の第7又は第8の特徴における前記各端末が、前記端末情報蓄積手段に蓄積された前記端末情報を、前記個別秘密情報端末蓄積手段に蓄積された前記個別秘密情報を用いて暗号化をして第2の署名情報を作成する第2の署名情報作成手段と、前記センタに対して前記共通秘密情報を含む前記第2のレポートの送信要求を行うために、前記第2の署名情報作成手段で作成された前記第2の署名情報を含むメッセージである第2のリクエストを作成し、前記センタに前記通信網を介して送信する第2のリクエスト作成送信手段とを有してなる個別秘密情報共有通信システム装置の構成採用にある。

【0045】本発明装置の第10の特徴は、上記本発明装置の第9の特徴における前記センタが、前記端末から送信される前記第2のリクエストを受信し、当該第2のリクエストに含まれる前記署名情報を取出す第2のリクエスト受信解析手段と、前記個別秘密情報センタ蓄積手段に蓄積された前記個別秘密情報を用いて復号化をして、前記第2のリクエスト受信解析手段で取出された前

記第2の署名情報に含まれる前記端末情報を取出し、当該第2の署名情報の正当性を認証した結果である第2の認証結果を作成する第2の署名情報認証手段とを有し、前記共通秘密情報送信指示手段が、前記第2の署名情報認証手段で作成された前記第2の認証結果が正常の場合に、前記第2の署名情報認証手段で取出された前記端末情報に示される端末への第2のレポートの送信指示を前記第2のレポート作成送信手段に対して行う機能を有してなる個別秘密情報共有通信システム装置の構成採用にある。

【0046】本発明装置の第11の特徴は、上記本発明装置の第9又は第10の特徴における前記各端末が、前記第2の署名情報を作成する度に毎回異なる値である第2の署名識別子を作成する第2の署名識別子作成手段を有し、前記第2の署名情報作成手段が、前記端末情報蓄積手段に蓄積された前記端末情報と、前記第2の署名識別子作成手段で作成された前記第2の署名識別子とを、前記個別秘密情報端末蓄積手段に蓄積された前記個別秘密情報を用いて暗号化して、前記第2の署名情報を作成する機能を有してなる個別秘密情報共有通信システム装置の構成採用にある。

【0047】本発明装置の第12の特徴は、上記本発明装置の第11の特徴における前記第2の署名情報認証手段が、前記個別情報センタ蓄積手段に蓄積された前記個別秘密情報を用いて復号化して、前記第2のリクエスト情報受信解析手段で取出された前記第2の署名情報から前記端末情報及び前記第2の署名識別子を取り出し前記第2の署名情報の正当性を認証した第2の認証結果を作成する機能を有し、前記センタが、前記第2の署名情報認証手段で取出された前記第2の署名識別子が過去に既に使用済みか否かを示す結果である第2の確認結果を作成する第2の署名識別子使用状況確認手段を有し、前記共通秘密情報送信指示手段が、前記第2の署名情報認証手段で作成された前記第2の認証結果が正常でかつ、前記第2の署名識別子使用状況確認手段で取出された前記第2の確認結果が未使用の場合に、前記第2の署名識別子使用状況確認手段で取出された前記端末情報に示される端末への前記第2のレポートの送信指示を、前記第2のレポート作成送信手段に対して行う機能を有してなる個別秘密情報共有通信システム装置の構成採用にある。

【0048】本発明装置の第13の特徴は、上記本発明装置の第1、第2、第3、第4、第5又は第6の特徴における前記個別秘密情報送信指示手段が、前記共通秘密情報の前記各端末への送信指示を行う機能も有し、前記第1のレポート作成送信手段が、当該個別秘密情報送信指示手段からの送信指示に従い、前記共通秘密情報センタ蓄積手段に蓄積された前記共通秘密情報を、前記個別秘密情報センタ蓄積手段に蓄積された前記個別秘密情報で暗号化する暗号化共通秘密情報を含むメッセージである第2のレポートを作成し前記各端末に前記通信網を介

して送信する機能も有してなる個別秘密情報共有通信システム装置の構成採用にある。

【0049】本発明装置の第14の特徴は、上記本発明装置の第13の特徴における前記第1のレポート受信解析手段が、前記センタから送信される前記第2のレポートを受信し当該第2のレポートに含まれる前記暗号化共通秘密情報を、前記個別秘密情報端末蓄積手段に蓄積された前記個別秘密情報で復号化し前記共通秘密情報を取出すとともに、当該共通秘密情報の受信が正常完了したか否かを示す結果である第2のレポート受信結果を作成する機能も有し、前記共通秘密情報消去手段が、当該第1のレポート受信解析手段で作成された前記第2のレポート受信結果が正常を意味する場合に、前記個別秘密情報端末蓄積手段で蓄積している前記個別秘密情報を消去する機能も有し、前記共通秘密情報端末蓄積手段が、前記第1のレポート受信解析手段で取出された前記共通秘密情報を蓄積する機能も有してなる個別秘密情報共有通信システム装置の構成採用にある。

【0050】本発明装置の第15の特徴は、上記本発明装置の第13又は第14の特徴における前記第1の署名情報作成手段が、前記端末情報蓄積手段に蓄積された前記端末情報を、前記個別秘密情報端末蓄積手段に蓄積された前記個別秘密情報とを用いて暗号化して第2の署名情報を作成する機能も有し、前記第1のリクエスト作成送信手段が、前記センタに対して前記共通秘密情報を含む前記第2のレポートの送信要求を行うために、前記第2の署名情報作成手段で作成された前記第2の署名情報を含むメッセージである第2のリクエストを作成し、前記センタに前記通信網を介して送信する機能も有してなる個別秘密情報共有通信システム装置の構成採用にある。

【0051】本発明装置の第16の特徴は、上記本発明装置の第15の特徴における前記第1のリクエスト受信解析手段が、前記端末から送信される前記第2のリクエストを受信し、当該第2のリクエストに含まれる前記署名情報を取出す機能も有し、第1の署名情報認証手段が、前記個別秘密情報センタ蓄積手段に蓄積された前記個別秘密情報を用いて、前記第2のリクエスト受信解析手段で取出された前記第2の署名情報に含まれる前記端末情報を取出し、当該第2の署名情報の正当性を認証した結果である第2の認証結果を作成する機能も有し、前記個別秘密情報送信指示手段が、前記第1の署名情報認証手段で作成された前記第2の認証結果が正常の場合に、前記第1の署名情報認証手段で取出された前記端末情報に示される端末への第2のレポートの送信指示を前記第1のレポート作成送信手段に対して行う機能も有してなる個別秘密情報共有通信システム装置の構成採用にある。

【0052】本発明装置の第17の特徴は、上記本発明装置の第15又は第16の特徴における前記第1の署名

識別子作成手段が、前記第2の署名情報を作成する度に毎回異なる値である第2の署名識別子を作成する機能も有し、前記第1の署名情報作成手段が、前記端末情報蓄積手段に蓄積された前記端末情報と、前記第2の署名識別子作成手段で作成された前記第2の署名識別子とを、前記個別秘密情報端末蓄積手段に蓄積された前記個別秘密情報を用いて暗号化をして、前記第2の署名情報を作成する機能も有してなる個別秘密情報共有通信システム装置の構成採用にある。

【0053】本発明装置の第18の特徴は、上記本発明装置の第17の特徴における前記第1の署名情報認証手段が、前記個別情報センタ蓄積手段に蓄積された前記個別秘密情報を用いて復号化をして、前記第1のリクエスト情報受信解析手段で取出された前記第2の署名情報から前記端末情報及び前記第2の署名識別子を取り出し前記第2の署名情報の正当性を認証した第2の認証結果を作成する機能も有し、前記第1の署名識別子使用状況確認手段が、前記第1の署名情報認証手段で取出された前記第2の署名識別子が過去に既に使用済みか否かを示す結果である第2の確認結果を作成する第2の署名識別子使用状況確認手段を有し、前記個別秘密情報送信指示手段が、前記第1の署名情報認証手段で作成された前記第2の認証結果が正常でかつ、前記第1の署名識別子使用状況確認手段で取出された前記第2の確認結果が未使用の場合に、前記第1の署名識別子使用状況確認手段で取出された前記端末情報に示される端末への前記第2のレポートの送信指示を、前記第2のレポート作成送信手段に対して行う機能も有してなる個別秘密情報共有通信システム装置の構成採用にある。

【0054】本発明装置の第19の特徴は、上記本発明装置の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10、第11、第12、第13、第14、第15、第16、第17又は第18の特徴における前記通信網が、LANや、電話及びISDNを含む公衆通信回線のうちの少なくとも1つからなる個別秘密情報共有通信システム装置の構成採用にある。

【0055】本発明装置の第20の特徴は、上記本発明装置の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10、第11、第12、第13、第14、第15、第16、第17、第18又は第19の特徴における前記センタが、前記共通秘密情報及び前記個別秘密情報を共有しセキュリティ通信を行うセキュリティ通信部を有してなる個別秘密情報共有通信システム装置の構成採用にある。

【0056】本発明装置の第21の特徴は、上記本発明装置の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10、第11、第12、第13、第14、第15、第16、第17、第18又は第19の特徴における前記センタとは別に、前記共通秘密情報及び前記個別秘密情報を共有しセキュリティ通信を行うセキュリティ

通信装置を設けてなる個別秘密情報共有通信システム装置の構成採用にある。

【0057】本発明装置の第22の特徴は、上記本発明装置の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10又は第11の特徴における前記センタ及び前記各端末が、別に、前記共通秘密情報を時間関数及び設定自在なパラメータとする世代識別子の関数を入力及び蓄積する鍵注入器を設けてなる個別秘密情報共有通信システム装置の構成採用にある。

【0058】本発明装置の第23の特徴は、上記本発明装置の第5、第6、第7、第8、第9、第10、第11、第12、第13、第14、第15、第16、第17、第18、第19、第20、第21又は第22の特徴における前記第1の署名識別子作成手段が、前記第1の署名情報を作成する度にカウントアップするカウンタ及び乱数を発生するプログラムのうちの1つを有してなる個別秘密情報共有通信システム装置の構成採用にある。

【0059】本発明装置の第24の特徴は、上記本発明装置の第11、第12、第17、第18、第19、第20、第21、第22又は第23の特徴における前記第2の署名識別子が、前記第2の署名情報を作成する度にカウントアップするカウンタ及び乱数を発生するプログラムのうちの1つを有してなる個別秘密情報共有通信システム装置の構成採用にある。

【0060】

【発明の実施の形態】以下、添付図面を参照して、本発明の一実施形態に係る方法例及びこれに対応する装置例につき順に説明する。

【0061】(装置例)本装置例を図1乃至図5を参照して説明する。図1は、本装置例の個別秘密情報共有通信システム装置を示す全体構成図であり、図2は、個別秘密情報共有通信システム装置のセンタの内部構成ブロック図であり、図3は、個別秘密情報共有通信システム装置の端末の内部構成ブロック図であり、図4は、センタと端末との間での通信を示す説明図であり、図5は、センタと端末との間及び各端末間での通信を示す説明図である。

【0062】本装置例の個別秘密情報共有通信システム装置 α は、共通秘密情報P及び個別秘密情報S1～Sk(kは任意の自然数)を共有するセンタ1と、センタ1から共有秘密情報P及び各個別秘密情報S1～Skを取寄せる端末2-1～2-kと、センタ1と各端末2-1～2-kとを接続しLAN又は電話、ISDN等の公衆通信回線等である通信網3とを有する。センタ1と端末2-1～2-kとの間に新しく通信回線を設ける必要はない。

【0063】センタ1は、図4乃至図5に示すよう、個別秘密情報S1～Skを各端末2-1～2-kへ送信する個別秘密情報払い出し部4と、各端末2-1～2-kとセキュリティ通信を行うセキュリティ通信部5とを有

する。

【0064】また、図2及び図3においては、センタ1と全端末2-1～2-k中の端末2-kとの間の接続による端末2-kの構成を説明したものであり、他の端末2-1～2-(k-1)についても端末2-kと同様の構成を採る。よって、ここでは、端末2-kと接続されたセンタ1及び端末2-kの構成を代表して説明する。

【0065】個別秘密情報払い出し部4は、共通秘密情報Pを蓄積する共通秘密情報センタ蓄積手段6と、全端末2-1～2-kの個別秘密情報S1～Skを蓄積する個別秘密情報センタ蓄積手段7と、各端末2-1～2-kからの署名情報a1を有するリクエストb1を受信し署名情報a1を取出すリクエスト受信解析手段8と、リクエスト受信解析手段8からの署名情報a1から端末情報ID及び署名識別子R1を取出し認証を行い認証結果c1を作成する署名情報認証手段9と、署名情報認証手段9からの署名識別子R1の使用状況から確認結果d1を作成する署名識別子使用状況確認手段10と、署名情報認証手段9からの認証結果c1及び署名識別子使用状況確認手段10からの確認結果d1により個別秘密情報Skの送信指示を行う個別秘密情報送信指示手段11と、個別秘密情報送信指示手段11からの送信指示によりレポートe1を作成し各端末2-1～2-kへ送信するレポート作成送信手段12とを有する。

【0066】また他に、各端末2-1～2-kからの署名情報a2を有するリクエストb2を受信し署名情報a2を取出すリクエスト受信解析手段13と、リクエスト受信解析手段13からの署名情報a2から端末情報ID及び署名識別子R2を取出し認証を行い認証結果c2を作成する署名情報認証手段14と、署名情報認証手段14からの署名識別子R2の使用状況から確認結果d2を作成する署名識別子使用状況確認手段15と、署名情報認証手段14からの認証結果c2及び署名識別子使用状況確認手段15からの確認結果d2により共通秘密情報Pの送信指示を行う共通秘密情報送信指示手段16と、共通秘密情報送信指示手段16からの送信指示によりレポートe2を作成し各端末2-1～2-kへ送信するレポート作成送信手段17とを有する。

【0067】端末2-kは、端末情報IDを蓄積する端末情報蓄積手段18と、署名識別子R1を作成する署名識別子作成手段19と、共通秘密情報Pを蓄積する共通秘密情報蓄積手段20と、共通秘密情報蓄積手段20からの共通秘密情報Pを用いて端末情報蓄積手段18からの端末情報ID及び署名識別子作成手段19からの署名識別子R1から署名情報a1を作成する署名情報作成手段21と、署名情報作成手段21からの署名情報a1からリクエストb1を作成及びセンタ1へ送信するリクエスト作成送信手段22と、センタ1からのレポートe1を受信し個別秘密情報Skを取出してレポート受信結果h1を作成するレポート受信解析手段23と、レポート

受信解析手段23からの個別秘密情報Skを蓄積する個別秘密情報端末蓄積手段24と、レポート受信解析手段23からのレポート受信結果h1により共通秘密情報蓄積手段20の共通秘密情報Pを消去する共通秘密情報消去手段25とを有する。

【0068】また他に、署名識別子R2を作成する署名識別子作成手段26と、個別秘密情報蓄積手段24からの個別秘密情報Skを用いて端末情報蓄積手段18からの端末情報ID及び署名識別子作成手段26からの署名識別子R1から署名情報a2を作成する署名情報作成手段27と、署名情報作成手段27からの署名情報a2からリクエストb2を作成及びセンタ1へ送信するリクエスト作成送信手段28と、センタ1からのレポートe2を受信し共通秘密情報Pを取出しレポート受信結果h2を作成するレポート受信解析手段29と、レポート受信解析手段29からのレポート受信結果h2により個別秘密情報蓄積手段24の個別秘密情報Skを消去する個別秘密情報消去手段30とを有する。

【0069】なお、図4は、センタ1と各端末2-1～2-kとの間で通信を行う場合であり、秘密情報センタ蓄積エリア31aは、センタ1において、共通秘密情報P及び個別情報秘密情報S1～Skを蓄積し、共通秘密情報センタ蓄積手段6及び個別秘密情報センタ蓄積部7に相当し、秘密情報端末蓄積エリア32a-1～32a-kは、各端末2-1～2-kにおいて、共通秘密情報P及び個別情報秘密情報S1～Skのそれぞれを蓄積し、共通秘密情報端末蓄積手段20及び個別秘密情報端末蓄積部24に相当する。

【0070】また、図5は、センタ1と各端末2-1～2-kとの間及び各端末2-1～2-k間で通信を行う場合であり、秘密情報センタ蓄積エリア31bは、センタ1において、共通秘密情報P、個別情報秘密情報S1～Sk及び端末2-pから端末2-qへの秘密情報である端末間秘密情報Sp、q (p, q=1～k, p≠q)を蓄積し、秘密情報蓄積エリア32b-1～32b-kは、例えば、端末2-kにおいて、共通秘密情報P及び個別情報秘密情報Sk、1～Sk、(k-1)を蓄積する。なお、Sp、q=Sq、pとしてもよい。

【0071】また、図4及び図5で示すように、センタ1は、一般に個別秘密情報払い出し部4とセキュリティ通信部5で構成されることができ、この二つは1つの装置である必要はなく、セキュリティ強度の高い通信回線で接続された別の装置で構成されてもよいことは言うまでもない。

【0072】また、センタ1において、リクエスト受信解析手段13、署名情報認証手段14、署名識別子使用状況確認手段15、共通秘密情報送信指示手段16、レポート作成送信手段17は、順にそれぞれ、リクエスト受信解析手段8、署名情報認証手段9、署名識別子使用状況確認手段10、個別秘密情報送信指示手段11、レ

ポート作成送信手段12と同様の構成で実現可能であるから、それぞれ二つを時間的に切替えて共用することもできる。

【0073】同じく、端末2-kにおいて、署名識別子作成手段26、署名情報作成手段27、リクエスト作成送信手段28、レポート受信解析手段29、個別秘密情報消去手段30は、順にそれぞれ、署名識別子作成手段19、署名情報作成手段21、リクエスト作成送信手段22、レポート受信解析手段23、共通秘密情報消去手段25と同様の構成で実現可能であるから、それぞれ二つを時間的に切替えて共用することもできる。

【0074】(方法例) 本方法例は、前記装置例に適用したものであり、同じく図1乃至図5と、他に図6及び図7を参照して説明する。図6は、本方法例のステップ1におけるリクエストb1の形成を示す説明図であり、図7は、本方法例のステップ4におけるリクエストb2の形成を示す説明図である。

【0075】また、本方法例の手順をステップ1乃至ステップ5に分けて順に説明する。ステップ1及びステップ2は、在庫状態であった端末が運用(セキュリティ通信)を開始するために設置時等の事前に行われる。ステップ3は、運用(セキュリティ通信)を行う段階である。ステップ4及びステップ5は、運用段階にあった端末を一旦撤去し、(将来の設置のために)在庫状態にする必要がある場合等に行われるものである。以下、全端末2-1~2-kのうちの端末2-kと、センタ1との間での手順を説明するが、他の端末も同様の手順で行われる。

【0076】なお、ステップ1、2、4、5は、センタ1の個別秘密情報払い出し部4と端末2-kとの間の手順であり、ステップ3は、センタ1のセキュリティ通信部5と端末2-kとの間の手順である。

【0077】<ステップ1>ステップ1は、端末2-kからセンタ1へ個別秘密情報Skの受信要求(リクエストb1)を行う手順である。センタ1から個別秘密情報Skの送信を自発的にいき、端末2-kから受信要求を行う必要が無い場合には、当該ステップ1は必要無い。

【0078】先ず、端末2-kにおいて、端末情報蓄積手段18に、センタ1が全端末2-1~2-kの中で当該端末2-kを識別可能な端末情報IDを蓄積する。端末情報IDとしては、端末2-k自身が接続されている通信回線のアドレス情報や、センタ1が割り振った連続番号等を使用することが可能であるが、各端末2-1~2-kで重複しないものでなくてはならない。また、端末情報IDの入力方法の一具体例としては、設置時に作業者が、前記接続されている通信回線のアドレス等を入力する方法等がある。

【0079】また、署名識別子作成手段19によって、署名識別子R1を作成する。署名識別子R1は、署名情報作成手段21で署名情報a1を作成する度に異なる値

であるものであり、具体的には、署名情報作成手段21で署名情報a1を作成する度にカウントアップするカウンタや、乱数を生成するプログラム等で実現することが可能である。

【0080】また、予め共通秘密情報端末蓄積手段20によって、及びセンタ1の共通秘密情報センタ蓄積手段6によって、共に共通の共通秘密情報Pを蓄積する。共通秘密情報Pは、予めセンタ1と全端末2-1~2-kとの間で共有しておかなければならないが、共通秘密情報Pは全端末2-1~2-kで共通な情報であることから、端末2-kの製造段階でセンタ1が指定した情報を全端末2-1~2-kの不揮発性メモリ等の情報蓄積媒体に予め書き込んでおくことで容易に実現可能である。

【0081】そして、署名情報作成手段21によって、端末情報蓄積手段18に蓄積された端末情報IDと署名識別子作成手段19で作成された署名識別子R1とを、共通秘密情報端末蓄積手段20からの共通秘密情報Pを用いて、センタ1に送信する署名情報a1を作成する。

【0082】署名情報a1の作成処理の一具体例としては、図6に示すように予め指定された暗号化関数fを用いて、端末情報IDと署名識別子R1を、共通秘密情報Pを暗号鍵として暗号化したデータf_p(ID, R1)を、端末情報ID及び署名識別子R1と一緒に送信する方法が考えられる。

【0083】署名情報a1の作成処理では、暗号化関数fの入力値と出力値が通信網3上に現れることから、通信網3上のモニタ信号から共通秘密情報Pを推測することが事実上不可能とするためには、暗号化関数fに、暗号化した情報と元の情報から暗号を求める既知平文攻撃への十分な耐性を有するものを用いることが望ましい。また、ここでは暗号鍵を共通秘密情報Pとして説明したが、実際には暗号化関数fと暗号鍵の組合せ自体が暗号鍵と考えることもできる。

【0084】上記のように、端末情報IDと署名識別子R1を組合せたものを、共通秘密情報Pで処理したものを署名情報a1として用いることにより、センタ1が受信するリクエストb1に含まれる署名情報a1として、同一内容のリクエストb1が2回以上使用されないことが保障される。よって、不正者が、過去に使用されたリクエストb1を通信網3上でモニタしたものを、不正アクセス時に送信する信号としてそのまま用いたとしても、センタ1ではこれを検出し排除することが可能となる。

【0085】そして、リクエスト作成送信手段22によって、署名情報a1を含むリクエストb1を作成し、通信網3を介してセンタ1に送信する。通信網3の公衆通信回線を用いる場合のリクエストb1の送信の具体的な動作としては、先ず発呼動作を行いセンタ1との回線接続が完了した後、確保された通信チャネル上でリクエストb1メッセージの送信を行うこととなる。

【0086】次に、センタ1において、リクエスト受信解析手段8では、端末2-kのリクエスト作成送信手段22から通信回線を介して送信されたリクエストb1を受信して、含まれる署名情報a1を取出す。

【0087】そして、署名情報認証手段9によって、共通秘密情報センタ蓄積手段6に蓄積された共通秘密情報Pを用いて、リクエスト受信解析手段8で取出された署名情報a1に含まれる端末情報ID及び署名識別子R1を取出すとともに、署名情報a1の正当性を認証した結果である認証結果c1を作成する。

【0088】この署名情報a1からの認証処理の一具体例を以下に示す。ここで示す例は、上記に記載した、署名情報a1として図6に示すように予め指定された暗号化関数fを用いて端末情報IDと署名識別子R1を、共通秘密情報Pを暗号鍵として暗号化したものを、端末情報IDと署名識別子R1とを一緒に送信する場合に対応するものである。

【0089】署名情報認証手段9では、リクエスト受信解析手段8で取出された署名情報a1に含まれる暗号化データf_p (ID, R1)を、暗号化関数fと共通秘密情報センタ蓄積手段6に蓄積された共通秘密情報Pである暗号鍵を用いて復号化して得られた復号化端末情報ID'と復号化署名識別子R1'を、署名情報a1に含まれる端末情報ID及び署名識別子R1とそれぞれ比較し、一致するか否かをチェックする。当該チェックを行った結果、両者が一致した場合には、端末2-kが正規の共通秘密情報Pを具備しているものと判断できることから、認証結果c1を正常とする。

【0090】そして、署名識別子使用状況確認手段10によって、署名情報認証手段9で取出された端末情報IDに示される各端末毎に、過去に既に使用された署名識別子R1を管理し、署名情報認証手段9で取出された署名識別子R1が未使用か否かをチェックし、確認結果d1として作成する。

【0091】＜ステップ2＞ステップ2は、センタ1から端末2-kに対して個別秘密情報Skの送信を行う手順である。ステップ2は、本方法例において、必須の手順である。

【0092】先ず、センタ1において、個別秘密情報送信指示手段11によって、署名情報認証手段9で作成された認証結果c1が正常でかつ、署名識別子使用状況確認手段10で作成された確認結果d1が未使用の場合に、署名情報認証手段9で取出された端末情報IDに示される端末2-kへのレポートe1の送信指示をレポート作成送信手段12に対して行う。

【0093】また、予め個別秘密情報センタ蓄積手段7によって、各端末毎の個別秘密情報Skを蓄積する。個別秘密情報センタ蓄積手段7では、全端末2-1～2-kの分の個別秘密情報S1～Skを蓄積し、また個別秘密情報Skとして予め作成しておいたものを蓄積しても

良いし、必要に応じて作成して蓄積してもよいが、一旦端末2-1～2-kに送信済のものについては蓄積しておく必要がある。

【0094】個別秘密情報Sk及び共通秘密情報Pとしては、データの暗号化を行う場合には暗号鍵、認証を行う場合にはユーザ名やパスワード等を含むし、セキュリティ通信時に使用する通信回線やポートを特定する場合にはこれらの情報を含むこととなる。

【0095】そして、レポート作成送信手段12によって、個別秘密情報送信指示手段11からのレポートe1の送信指示に従い、個別秘密情報センタ蓄積手段7に蓄積された個別秘密情報Skを、共通秘密情報センタ蓄積手段6に蓄積された共通秘密情報Pで暗号化した暗号化個別秘密情報Sk'を含むメッセージであるレポートe1を作成し、端末2-kに通信網3を介して送信する。

【0096】次に、端末2-kにおいて、レポート受信解析手段23によって、センタ1のレポート作成送信手段12から送信されるレポートe1を受信し、レポートe1に含まれる暗号化個別秘密情報Sk'を、共通秘密情報端末蓄積手段20に蓄積された共通秘密情報Pで復号化し個別秘密情報Skを取出すとともに、個別秘密情報Skの受信が正常完了したか否かを示す結果であるレポート受信結果h1を作成する。

【0097】そして、個別秘密情報端末蓄積手段24によって、レポート受信解析手段23により取出された個別秘密情報Skを蓄積する。

【0098】そして、共通秘密情報消去手段25によって、レポート受信解析手段23で作成されたレポート受信結果h1が正常を意味する場合に、第三者が端末2-kから共通秘密情報Pを取出さないように、共通秘密情報端末蓄積手段20で蓄積している共通秘密情報Pを消去する。

【0099】＜ステップ3＞ステップ3は、端末2-kとセンタ1との間で個別秘密情報Skを用いてセキュリティ通信を行う手順である。具体的には個別秘密情報Skを暗号鍵として用いたり、認証に用いる以外にも実際に通信を行う際に用いるアドレスやポートを指定する情報として用いることもできる。

【0100】また、本方法例において、図4に示すようにセンタ1のセキュリティ通信部5と端末2-kとの間で通信網3を介してセキュリティ通信を行う際に用いる個別秘密情報S1～Skのみを共有する例を記述しているが、図5に示すようにセンタ1と端末2-kとの間だけでなく端末相互2-1～2-k間でセキュリティ通信を行うために用いる秘密情報である端末間秘密情報を個別秘密情報S1～Skに含めることも可能であることは言うまでもない。

【0101】この場合には、センタ1から端末2-kに送信されるレポートに含まれる個別秘密情報として、センタ1と端末2-kとの間の個別秘密情報Sk以外に

も、端末2-kから他の全端末への端末間秘密情報 S_k 、 q ($q=1\sim$ 全端末数 k ：但し k を除く)を含めておけばよい。

【0102】<ステップ4>ステップ4は、端末2-kからセンタ1へ共通秘密情報 P の受信要求(リクエスト b_1)を行う手順である。センタ1から共通秘密情報 P の送信を自発的に行い、端末2-kから受信要求を行う必要が無い場合にはステップ4は必要無く、また、端末2-kで共通秘密情報 P の再構築が必要ない場合にもステップ4は必要無い。

【0103】まず、端末2-kにおいて、署名識別子作成手段26によって、署名識別子 R_2 を作成する。署名識別子 R_2 は、署名情報作成手段27で署名情報 a_2 を作成する度に異なる値であるものであり、具体的には、署名情報作成手段27で署名情報 a_2 を作成する度にカウンタアップするカウンタや、乱数を生成するプログラム等で実現することが可能である。

【0104】そして、署名情報作成手段27によって、端末情報蓄積手段18に蓄積された端末情報 ID と署名識別子作成手段26で作成された署名識別子 R_2 とを、個別秘密情報端末蓄積手段24からの個別秘密情報 S_k を用いて、センタ1に送信する署名情報 a_2 を作成する。

【0105】署名情報 a_2 の作成処理の一具体例としては、図7に示すように予め指定された暗号化関数 g を用いて、端末情報 ID と署名識別子 R_2 を、個別秘密情報 S_k を暗号鍵として暗号化したデータ $g_{S_k}(ID, R_2)$ を、端末情報 ID 及び署名識別子 R_2 と一緒に送信する方法が考えられる。

【0106】当該署名情報 a_2 の作成処理では、暗号化関数 g の入力値と出力値が通信網3上に現れることから、通信網3上のモニタ信号から個別秘密情報 S_k を推測することが事実上不可能とするためには、暗号化関数 g に既知平文攻撃への十分な耐性を有するものを用いることが望ましい。また、ここでは暗号鍵を個別秘密情報 S_k として説明したが、実際には暗号化関数 g と暗号鍵の組合せ自体が暗号鍵と考えることもできる。

【0107】上記のように、端末情報 ID と署名識別子 R_2 を組合せたものを、個別秘密情報 S_k で処理したものを署名情報 a_2 として用いることにより、センタ1が受信するリクエスト b_2 に含まれる署名情報 a_2 として、同一内容のリクエスト b_2 が2回以上使用されることが保障される。よって、不正者が、過去に使用されたリクエスト b_2 を通信網3上でモニタしたものを、不正アクセス時に送信する信号としてそのまま用いたとしても、センタ1ではこれを検出し排除することが可能となる。

【0108】そして、リクエスト作成送信手段28によって、署名情報 a_2 を含むリクエスト b_2 を作成し、通信網3を介してセンタ1に送信する。

【0109】次に、センタ1において、リクエスト受信解析手段13では、端末2-kのリクエスト作成送信手段28から通信網3を介して送信されたリクエスト b_2 を受信して、含まれる署名情報 a_2 を取出す。

【0110】そして、署名情報認証手段14によって、個別秘密情報センタ蓄積手段7に蓄積された個別秘密情報 S_k を用いて、リクエスト受信解析手段13で取出された署名情報 a_2 に含まれる端末情報 ID 及び署名識別子 R_2 を取出すとともに、署名情報 a_2 の正当性を認証した結果である認証結果 c_2 を作成する。

【0111】この署名情報 a_2 の認証処理の一具体例を以下に示す。ここで示す例は、上記に記載した、署名情報 a_2 として図7に示すように予め指定された暗号化関数 g を用いて端末情報 ID と署名識別子 R_2 を、個別秘密情報 S_k を暗号鍵として暗号化したものを、端末情報 ID と署名識別子 R_2 と一緒に送信する場合に対応するものである。

【0112】署名情報認証手段14では、リクエスト受信解析手段13で取出された署名情報 a_2 に含まれる暗号化データ $g_{S_k}(ID, R_2)$ を、暗号化関数 g と個別秘密情報センタ蓄積手段7に蓄積された個別秘密情報 S_k である暗号鍵を用いて復号化して得られた復号化端末情報 ID' と復号化署名識別子 R_2' を、署名情報 a_2 に含まれる端末情報 ID 及び署名識別子 R_2 とそれぞれ比較し、一致するか否かをチェックする。当該チェックを行った結果、両者が一致した場合には、端末2-kが正規の個別秘密情報 S_k を具備しているものと判断できることから、認証結果 c_2 を正常とする。

【0113】そして、署名識別子使用状況確認手段15によって、署名情報認証手段14で取出された端末情報 ID に示される各端末毎に、過去に既に使用された署名識別子 R_2 を管理し、署名情報認証手段9で取出された署名識別子 R_2 が未使用か否かをチェックし、確認結果 d_2 として作成する。

【0114】<ステップ5>ステップ5は、センタ1から端末2-kに対して共通秘密情報 P の送信を行う手順である。本方法例において、端末2-kで共通秘密情報 P の再構築が必要ない場合は、ステップ5は必要無い。

【0115】まず、センタ1において、共通秘密情報送信指示手段16によって、署名情報認証手段14で作成された認証結果 c_2 が正常でかつ、署名識別子使用状況確認手段15で作成された確認結果 d_2 が未使用の場合に、署名情報認証手段14で取出された端末情報 ID に示される端末2-kへのレポート e_2 の送信指示をレポート作成送信手段17に対して行う。

【0116】そして、レポート作成送信手段17によって、共通秘密情報送信指示手段16からのレポート e_2 の送信指示に従い、共通秘密情報センタ蓄積手段6に蓄積された共通秘密情報 P を、個別秘密情報センタ蓄積手段7に蓄積された個別秘密情報 S_k で暗号化した暗号化

共通秘密情報P'を含むメッセージであるレポートe2を作成し、端末2-kへ通信網3を介して送信する。

【0117】次に、端末2-kにおいて、レポート受信解析手段29によって、センタ1のレポート作成送信手段17から送信されるレポートe2を受信し、レポートe2に含まれる暗号化共通秘密情報P'を、個別秘密情報端末蓄積手段24に蓄積された個別秘密情報Skで復号化し共通秘密情報Pを取出すとともに、共通秘密情報Pの受信が正常完了したか否かを示す結果であるレポート受信結果h2を作成する。

【0118】そして、個別秘密情報消去手段30によって、レポート受信解析手段29で作成されたレポート受信結果h2が正常を意味する場合に、第三者が端末2-kから個別秘密情報Skを取出さないように、個別秘密情報端末蓄積手段24で蓄積している個別秘密情報Skを消去する。

【0119】以上述べてきた手順では、共通秘密情報Pは固定のものとして記述したが、万一何らかの原因で漏洩した場合にシステム全体のセキュリティ機能が停止することを考慮すると、これを防止するために予め容易に変更可能とすることが望ましい。

【0120】更新機能を具備する方法の一例としては、共通秘密情報Pを定数ではなく、時刻や日時等による時間関数とする方法が考えられる。具体的には、センタ1や端末2-kでは予め同期された時計機能を具備し、時計から通知される時間が随時変更されることにより、共通秘密情報Pは時間経過とともに自動的に変更することが可能となり、セキュリティ耐力は大幅に向上する。

【0121】しかし当該方法を用いた場合でも、共通秘密情報Pが時間関数である仕様そのものが漏洩した場合には、システム全体としてのセキュリティ機能が停止することになる。

【0122】これを解決する別の方法として、共通秘密情報Pをセンタ1及び各端末2-1~2-kにて何らかの形で入力可能な世代情報である世代識別子の関数とする方法が考えられる。当該世代識別子の入力方法としては、新たに端末を設置する段階で人手を介して入力する方法や、センタ1から予め通知しておく方法等が考えられる。この方法を用いることにより、万一ある世代の共通秘密情報Pが漏洩した場合にも、少なくとも新たな世代識別子に変更された端末については、セキュリティ機能を有効にすることができる。

【0123】また、前記世代識別子の関数を各端末2-1~2-kの内部に持たせるのではなく、各端末2-1~2-kのとは別の装置である鍵注入器に具備させ、人が世代情報を鍵注入器に入力し、その結果得られた出力値を各端末2-1~2-kに入力する方法を用いることにより、端末が盗難され内部解析されたような場合でも、波及効果を小さくすることができる。

【0124】以上、本発明の実施の形態につき説明した

が、本発明は、必ずしも上述した手段及び手法にのみ限定されるものではなく、本発明にいう目的を達成し、本発明にいう効果を有する範囲内において、適宜に変更実施することが可能なものである。

【0125】

【発明の効果】以上説明したように、本発明によれば、新しく通信回線を設置することなく、センタと各端末間で経済的に安価でかつ安全に個別秘密情報を共有することができ、また、共通秘密情報を変更可能なものにすれば、万一共通秘密情報が漏洩した場合にもシステム全体に影響が及ぶことがなくなる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係る個別秘密情報共有通信システム装置を示す全体構成図である。

【図2】同上、個別秘密情報共有通信システム装置のセンタの内部構成ブロック図である。

【図3】同上、個別秘密情報共有通信システム装置の端末の内部構成ブロック図である。

【図4】同上、センタと端末との間での通信を示す説明図である。

【図5】同上、センタと端末との間及び各端末間での通信を示す説明図である。

【図6】第1のリクエストの形成を示す説明図である。

【図7】第2のリクエストの形成を示す説明図である。

【符号の説明】

α…個別秘密情報共有通信システム装置

1…センタ

2-1~2-k…端末(k:任意の自然数)

3…通信網

4…個別秘密情報払い出し部

5…セキュリティ通信部

6…共通秘密情報センタ蓄積手段

7…個別秘密情報センタ蓄積手段

8, 13…リクエスト受信解析手段

9, 14…署名情報認証手段

10, 15…署名識別子使用状況確認手段

11…個別秘密情報送信指示手段

12, 17…レポート作成送信手段

16…共通秘密情報送信指示手段

18…端末情報蓄積手段

19, 26…署名識別子作成手段

20…共通秘密情報端末蓄積手段

21, 27…署名情報作成手段

22, 28…リクエスト作成送信手段

23, 29…レポート受信解析手段

24…個別秘密情報端末蓄積手段

25…共通秘密情報消去手段

30…個別秘密情報消去手段

31a, 31b…秘密情報センタ蓄積エリア

32a-1~32a-k, 32b-1~32b-k…秘

密情報端末蓄積エリア

ID…端末情報

R1, R2…署名識別子

P…共通秘密情報

S1~Sk…個別秘密情報

f, g…暗号化関数

a1, a2…署名情報

b1, b2…リクエスト

c1, c2…認証結果

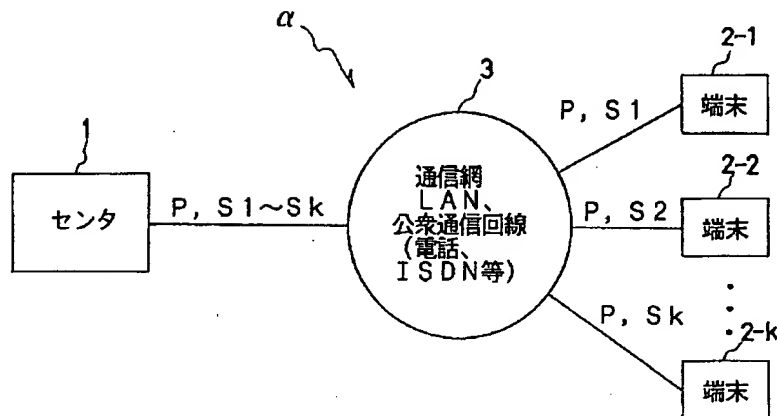
d1, d2…確認結果

e1, e2…レポート

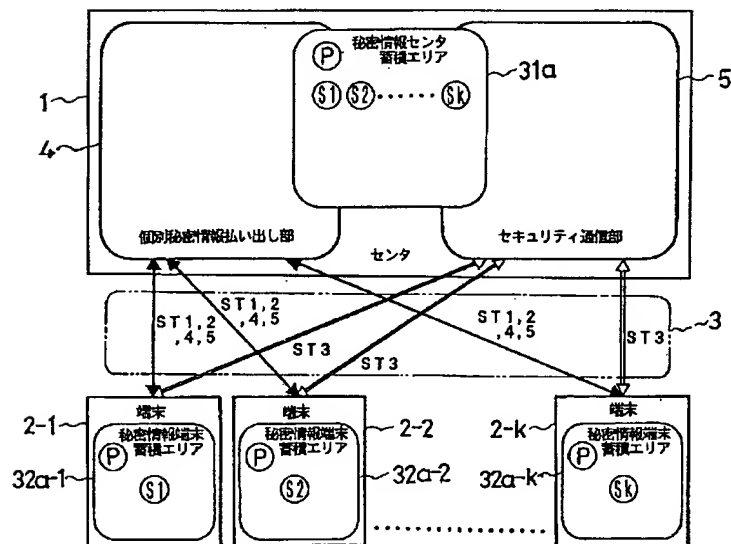
h1, h2…レポート受信結果

Sp, q…端末間秘密情報

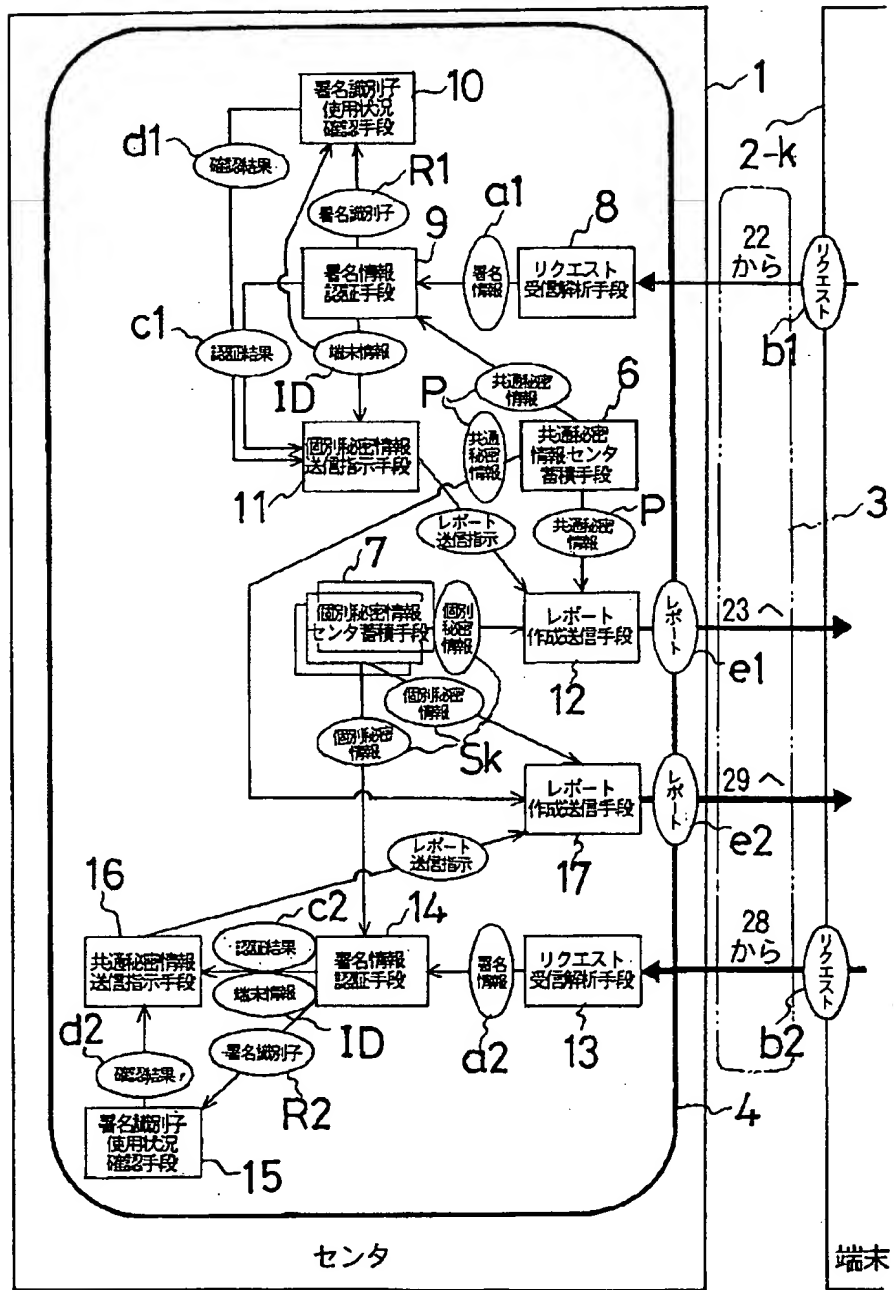
【図1】



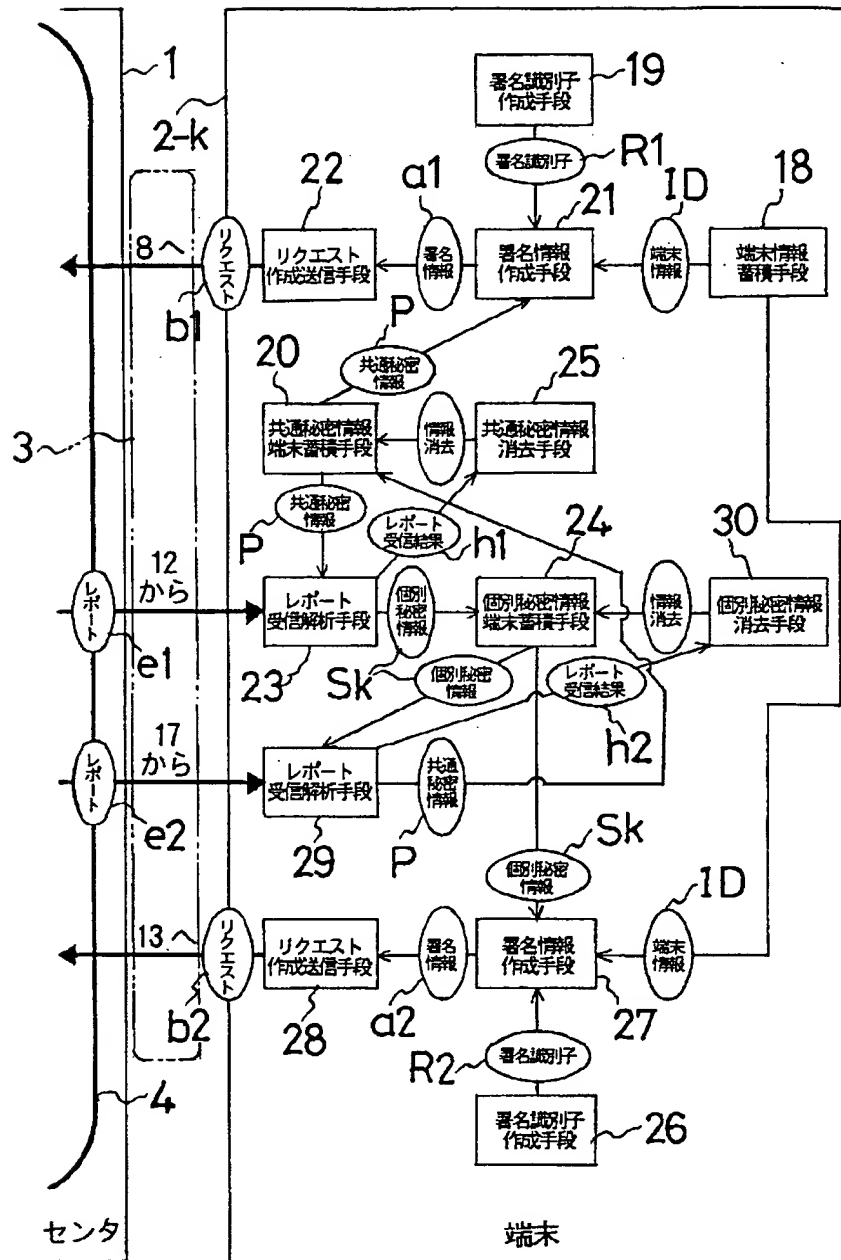
【図4】



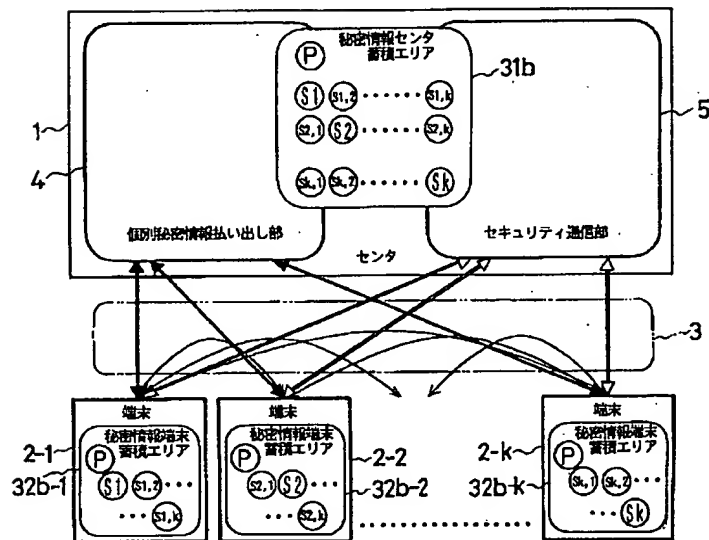
【図2】



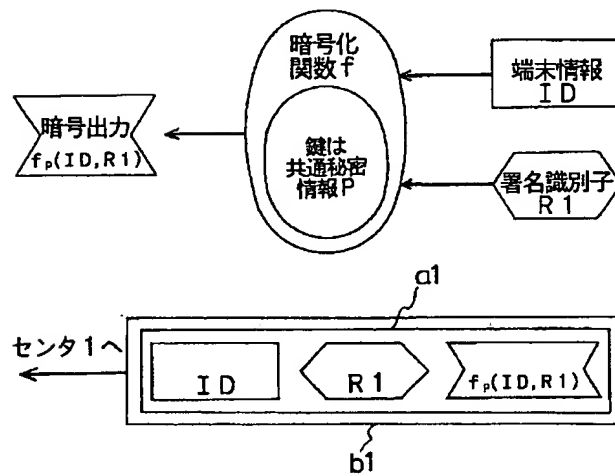
【図3】



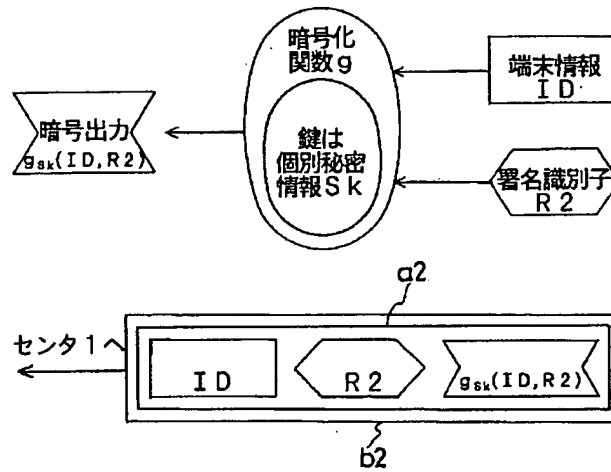
【図5】



【図6】



【図7】



フロントページの続き

(72)発明者 斉藤 隆一
東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72)発明者 中濱 清志
東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72)発明者 安永 健治
東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

Fターム(参考) 5K013 AA01 BA02 EA02 FA06